Part No. 208967-B
April 2000

4401 Great America Parkway
Santa Clara, CA 95052

Reference for the Passport 8000 Series Command Line Interface Routing Operations

NORTEL NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. April 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

Passport and NORTEL NETWORKS are trademarks of Nortel Networks.

Bay Networks is a registered trademark of Nortel Networks.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Taiwan Requirements

Bureau of Standards, Metrology and Inspection (BSMI) Statement

警告使用者:

這是甲類的資訊產品, 在居住的環境中使用時, 可能會造成射

頻干擾, 在這種情況下, 使用者會被要求採取某些適當的對策.

Canada Requirements Only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Passport 8000 Series routing switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Passport 8000 Series routing switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xxii
Text Conventions xxii
Related Publications xxiii
How to Get Help xxvi

Chapter 1
IP Routing and ARP Commands

IP Routing Commands 1-1
config ip Commands 1-1
show ip Commands 1-4
show ip forwarding Command 1-4
show ip interface Command 1-4
show ip route-discovery Command 1-4
show ip route info Command 1-5
show ip static-route info Command 1-5
config ethernet <ports> ip Commands 1-6
show ports info ip Command 1-8
Brouter Ports 1-8
show ports info brouter-port Command 1-9
vlan ip Commands 1-9
config vlan ip Commands 1-9
show vlan info ip Command 1-10
IP ARP Commands 1-10
config ip arp Commands 1-11
show ip arp info Command 1-12
config ethernet <ports> ip arp Commands 1-13
config ethernet <ports> ip Commands 1-13
show ports info arp Command 1-14

config vlan ip arp Commands 1-15
config vlan ip arp Command 1-15
show vlan info arp Command 1-16

Chapter 2
DHCP and UDP Commands

DHCP Relay Commands 2-1
config ip dhcp-relay Commands 2-2
show ip dhcp-relay Commands 2-3
show ip dhcp-relay fwd-path Command 2-3
show ip dhcp-relay counters Command 2-3
config ethernet <ports> ip dhcp-relay Commands 2-4
show ports dhcp-relay Commands 2-5
show ports info dhcp-relay Command 2-5
show ports stats dhcp-relay Command 2-5
config vlan <vid> ip dhcp-relay Commands 2-6
show vlan info dhcp-relay Command 2-7
UDP Commands 2-8
config ip udpfwd protocol Commands 2-8
config ip udpfwd portfwdlist Commands 2-9
config ip udpfwd interface Commands 2-9
show ip udpfwd Commands 2-10
show ip udpfwd interface info Command 2-10
show ip udpfwd portfwd info Command 2-10
show ip udpfwd portfwdlist info Command 2-11
show ip udpfwd protocol info Command 2-11

Chapter 3
RIP and OSPF Commands

RIP Commands 3-1
config ip rip Commands 3-1
show ip rip Commands 3-3
show ip rip info Command 3-3
show ip rip interface Command 3-4
config ethernet <ports> ip rip Commands 3-4
show ports info rip Command 3-7

config vlan <vid> ip rip Commands 3-8
show vlan info rip Command 3-10
OSPF Commands 3-10
config ip ospf Commands 3-10
config ip ospf Commands 3-11
config ip ospf host-route Commands 3-12
config ip ospf interface Commands 3-13
config ip ospf area Commands 3-15
config ip ospf area range Commands 3-16
config ip ospf area virtual-interface Commands 3-17
show ip ospf Commands 3-19
show ip ospf area Command 3-19
show ip ospf ase Command 3-19
show ip ospf default-metric Command 3-20
show ip ospf host-route Command 3-20
show ip ospf ifstats Command 3-21
show ip ospf info Command 3-21
show ip ospf interface Command 3-22
show ip ospf int-timers Command 3-22
show ip ospf lsdb Command 3-23
show ip ospf neighbors Command 3-25
show ip ospf range Command 3-26
show ip ospf stats Command 3-26
config ethernet <ports> ip ospf Commands 3-27
show ports ospf Commands 3-29
show ports error ospf Command 3-29
show ports info ospf Command 3-30
show ports stats ospf main Command 3-30
show ports stats ospf extended Command 3-31
config vlan <vid> ip ospf Commands 3-31
show vlan info ospf Command 3-33

Chapter 4
VRRP Commands

VRRP Commands 4-1
config ethernet <ports> ip vrrp Commands 4-1
show port vrrp Commands 4-3
show ports info vrrp main Command 4-3
show ports info vrrp extended Command 4-3
show ports stats vrrp Command 4-3
config vlan <vid> ip vrrp Commands 4-4
show vlan vrrp Commands 4-5
show vlan info vrrp main Command 4-5
show vlan info vrrp extended Command 4-6
show ip vrrp Commands 4-6
show ip vrrp info Command 4-6
show ip vrrp stats Command 4-7

Chapter 5
IP Multicast Commands

IP Multicast Commands 5-1
config ip mroute Commands 5-1
show ip mroute Commands 5-2
show ip mroute interface Command 5-2
show ip mroute next-hop Command 5-2
show ip mroute route Command 5-3
show ports stats routing Command 5-3
DVMRP Commands 5-4
config ip dvmrp Commands 5-4
config ip dvmrp Commands 5-4
config ip dvmrp interface Commands 5-6
show ip dvmrp Commands 5-6
show ip dvmrp info Command 5-6
show ip dvmrp interface Command 5-7
show ip dvmrp neighbor Command 5-8
show ip dvmrp next-hop Command 5-8
show ip dvmrp route Command 5-9
config ethernet <ports> ip dvmrp Commands 5-9

show ports info dvmrp Command 5-10
config vlan <vid> ip dvmrp Commands 5-11
show vlan info dvmrp Command 5-12
Layer 3 IGMP Commands 5-12
config ip l3-igmp Commands 5-13
config ip l3-igmp interface Commands 5-13
show ip l3-igmp Commands 5-14
show ip l3-igmp cache Command 5-14
show ip l3-igmp group Command 5-14
show ip l3-igmp interface Command 5-15
config ethernet <ports> ip l3-igmp Commands 5-16
show ports info l3-igmp Command 5-17
config vlan <vid> ip l3-igmp Commands 5-18
show vlan info l3-igmp Command 5-19

Chapter 6
IPX Commands

IPX Commands 6-1
config ipx Commands 6-2
config vlan <vid> ipx Commands 6-4
config ipx set Commands 6-4
config ipx static-route Commands 6-6
config ipx rip Commands 6-7
config ipx rip info Command 6-7
config ipx rip default Commands 6-7
config ipx rip Commands 6-8
config ipx sap Commands 6-8
config ipx sap info Command 6-8
config ipx sap default Commands 6-9
config ipx sap Commands 6-10

show ipx Commands 6-11
show ipx config Command 6-11
show ipx default Command 6-12
show ipx route Command 6-12
show ipx sap Command 6-13
show ipx stats Command 6-14
show vlan info ipx Command 6-15

Chapter 7
Policies Commands

IP Policies 7-1
config ip policy Commands 7-1
config ip policy addrlist Commands 7-2
config ip policy netlist Commands 7-3
config ip policy ospf Commands 7-4
config ip policy ospf accept Commands 7-4
config ip policy ospf announce Commands 7-6
config ip policy rip Commands 7-8
config ip policy rip accept Commands 7-8
config ip policy rip announce Commands 7-10
show ip policy Commands 7-12
show ip policy addrlist info Command 7-12
show ip policy netlist info Command 7-13
show ip policy ospf accept info Command 7-13
show ip policy ospf accept lists Command 7-14
show ip policy ospf accept match network Command 7-14
show ip policy ospf announce info Command 7-15
show ip policy ospf announce lists Command 7-15
show ip policy ospf announce match network Command 7-16
show ip policy rip accept info Command 7-16
show ip policy rip accept lists Command 7-17
show ip policy rip accept match network Command 7-17
show ip policy rip announce info Command 7-18
show ip policy rip announce lists Command 7-18
show ip policy rip announce match network Command 7-18

Chapter 8
IP QoS and Traffic Filter Commands

IP QoS Commands 8-1
config qos Commands 8-3
show qos queue Command 8-4
IP Traffic Filters 8-5
config ip traffic-filter Commands 8-6
config ip traffic-filter Commands 8-6
config ip traffic-filter create Commands 8-7
config ip traffic-filter filter Commands 8-8
config ip traffic-filter filter <fid> action Commands 8-8
config ip traffic-filter filter <fid> match Commands 8-9
config ip traffic-filter filter <fid> modify Commands 8-11
config ip traffic-filter global-set Commands 8-13
config ip traffic-filter set Commands 8-13
config ip traffic-filter traffic-profile <pid> Commands 8-14
Implementation of Rate Limiting in the Passport 8000 Series Switch 8-15
config ethernet <ports> ip traffic-filter Commands 8-18
show ip traffic-filter Commands 8-19
show ip traffic-filter active Command 8-19
show ip traffic-filter destination Command 8-19
show ip traffic-filter disabled Command 8-20
show ip traffic-filter enabled Command 8-20
show ip traffic-filter global Command 8-21
show ip traffic-filter info global-set Command 8-21
show ip traffic-filter info set Command 8-22
show ip traffic-filter interface Command 8-23
show ip traffic-filter source Command 8-23
show ip traffic-filter stats Command 8-24
show ip traffic-filter traffic-profile info Command 8-24

Appendix A
CLI Command List

Index

Figures

Figure 1-1. config ip info Command Output 1-3
Figure 1-2. config ip static-route info Command Output 1-3
Figure 1-3. show ip forwarding Command Output 1-4
Figure 1-4. show ip interface Command Output 1-4
Figure 1-5. show ip route info Command Output 1-5
Figure 1-6. show ip static-route info Command Output 1-6
Figure 1-7. config ethernet ip info Command Output 1-7
Figure 1-8. show ports info ip Command Output 1-8
Figure 1-9. show ports info brouter-port Command Output 1-9
Figure 1-10. config vlan ip info Command Output 1-10
Figure 1-11. show vlan info ip Command Output 1-10
Figure 1-12. config ip arp info Command (Partial Output) 1-12
Figure 1-13. show ip arp info Command Output 1-13
Figure 1-14. config ethernet ip arp-response info Command Output 1-14
Figure 1-15. show ports info arp Command (Partial Output) 1-14
Figure 1-16. config vlan ip proxy info Command Output 1-15
Figure 1-17. show vlan info arp Command Output 1-16

Figure 2-1. show ip dhcp-relay counters Command Output 2-3
Figure 2-2. config ethernet ip dhcp-relay info Command Output 2-4
Figure 2-3. show ports info dhcp-relay Command (Partial Output) 2-5
Figure 2-4. show ports stats dhcp-relay Command (Partial Output) 2-6
Figure 2-5. config vlan ip dhcp-relay info Command Output 2-7
Figure 2-6. show vlan info dhcp-relay Command Output 2-7
Figure 2-7. show ip udpfwd interface info Command Output 2-10
Figure 2-8. show ip udpfwd portfwd info Command Output 2-11
Figure 2-9. show ip udpfwd protocol info Command Output 2-12

Figure 3-1. config ip rip info Command Output 3-3
Figure 3-2. show ip rip Command Output 3-3
Figure 3-3. show ip rip interface Command Output 3-4
Figure 3-4. config ethernet ip rip info Command Output 3-6
Figure 3-5. show ports info rip Command (Partial Output) 3-7
Figure 3-6. config vlan ip rip info Command Output 3-9
Figure 3-7. show vlan info rip Command Output 3-10
Figure 3-8. config ip ospf info Command Output 3-12
Figure 3-9. config ip ospf interface info Command Output 3-15
Figure 3-10. config ip ospf area info Command Output 3-16
Figure 3-11. show ip ospf area Command Output 3-19
Figure 3-12. show ip ospf ase Command Output 3-20
Figure 3-13. show ip ospf default-metric Command Output 3-20
Figure 3-14. show ip ospf ifstats Command Output 3-21
Figure 3-15. show ip ospf info Command Output 3-21
Figure 3-16. show ip ospf interface Command Output 3-22
Figure 3-17. show ip ospf int-timers Command Output 3-22
Figure 3-18. show ip ospf lsdb Command Output 3-23
Figure 3-19. show ip ospf lsdb detail Command Output 3-25
Figure 3-20. show ospf neighbors Command Output 3-25
Figure 3-21. show ip ospf stats Command Output 3-26
Figure 3-22. config ethernet ip ospf info Command Output 3-29
Figure 3-23. show ports error ospf Command Output 3-29
Figure 3-24. show ports info ospf Command (Partial Output) 3-30
Figure 3-25. show ports stats ospf main Command Output 3-31
Figure 3-26. config vlan ip ospf info Command Output 3-33
Figure 3-27. show vlan info ospf Command Output 3-33

Figure 4-1. config ethernet ports ip vrrp info Command Output 4-2
Figure 4-2. show ports info vrrp extended Command Output 4-3
Figure 4-3. config vlan ip vrrp info Command Output 4-5
Figure 4-4. show vlan info vrrp main Command Output 4-5
Figure 4-5. show vlan info vrrp extended Command Output 4-6
Figure 4-6. show ip vrrp info Command Output 4-7

Figure 5-1. show ip mroute interface Command Output 5-2
Figure 5-2. show ip mroute next-hop Command Output 5-2
Figure 5-3. show ip mroute route Command Output 5-3
Figure 5-4. show ports stats routing Command (Partial Output) 5-4
Figure 5-5. config ip dvmrp info Command Output 5-6
Figure 5-6. show ip dvmrp info Command Output 5-7
Figure 5-7. show ip dvmrp interface Command Output 5-8
Figure 5-8. show ip dvmrp next-hop Command Output 5-9
Figure 5-9. show ip dvmrp route Command Output 5-9
Figure 5-10. config ethernet ip dvmrp info Command Output 5-10
Figure 5-11. show ports info dvmrp Command Output 5-11
Figure 5-12. config vlan ip dvmrp info Command Output 5-12
Figure 5-13. show vlan info dvmrp Command Output 5-12
Figure 5-14. show ip l3-igmp cache Command Output 5-14
Figure 5-15. show ip l3-igmp group Command Output 5-14
Figure 5-16. show ip l3-igmp interface Command Output 5-15
Figure 5-17. config ethernet ip l3-igmp info Command Output 5-17
Figure 5-18. show ports info 13-igmp Command (Partial Output) 5-17
Figure 5-19. config vlan ip l3-igmp info Command Output 5-19
Figure 5-20. show vlan info l3-igmp Command Output 5-19

Figure 6-1. config ipx set info Command Output 6-5
Figure 6-2. config ipx static-route info Command Output 6-6
Figure 6-3. show ipx config Command Output 6-11
Figure 6-4. show ipx default Command Output 6-12
Figure 6-5. show ipx route Command Output 6-12
Figure 6-6. show ipx sap Command Output 6-13
Figure 6-7. show ipx stats Command Output 6-14
Figure 6-8. show vlan info Command Output 6-15

Figure 7-1. config ip policy addrlist info Command Output 7-2
Figure 7-2. config ip policy netlist info Command Output 7-3
Figure 7-3. config ip policy ospf accept info Command Output 7-5
Figure 7-4. config ip policy ospf announce info Command Output 7-7
Figure 7-5. config ip policy rip accept info Command Output 7-9

Figure 7-6. config ip policy rip announce info Command Output 7-12
Figure 7-7. show ip policy addrlist info Command Output 7-13
Figure 7-8. show ip policy netlist info Command Output 7-13
Figure 7-9. show ip policy ospf accept info Command Output 7-14
Figure 7-10. show ip policy ospf accept lists Command Output 7-14
Figure 7-11. show ip policy ospf announce info Command Output 7-15
Figure 7-12. show ip policy ospf announce lists Command Output 7-15
Figure 7-13. show ip policy rip accept info Command Output 7-16
Figure 7-14. show ip policy rip accept lists Command Output 7-17
Figure 7-15. show ip policy rip accept match network Command Output 7-17

Figure 8-1. config qos info Command Output 8-4
Figure 8-2. show qos queue Command Output 8-5
Figure 8-3. config ip traffic-filter create info Command Output 8-7
Figure 8-4. config ip traffic-filter filter action info Command Output 8-9
Figure 8-5. config ip traffic-filter filter match info Command Output 8-11
Figure 8-6. config ip traffic-filter filter modify info Command Output 8-12
Figure 8-7. config ip traffic-filter global-set info Command Output 8-13
Figure 8-8. config ip traffic-filter set info Command Output 8-14
Figure 8-9. config ip traffic-filter traffic-profile info Command Output 8-18
Figure 8-10. show ip traffic-filter destination Command Output 8-20
Figure 8-11. show ip traffic-filter global Command Output 8-21
Figure 8-12. show ip traffic-filter info global-set Command Output 8-22
Figure 8-13. show ip traffic-filter info set Command Output 8-23
Figure 8-14. show ip traffic-filter interface Command Output 8-23
Figure 8-15. show ip traffic-filter stats Command Output 8-24
Figure 8-16. show ip traffic-filter traffic-profile Command Output 8-25

Tables

Table 3-1. RIP Supply and Listen Settings and Switch Action 3-6

Table A-1. CLI Command List A-1

Preface

The Nortel Networks™ Passport™ command line interface (CLI) is one method used to configure and manage a Passport 8000 Series switch. The CLI, as well as the Passport Management Software graphical user interface (GUI), allows you to set up, configure, and manage your Passport 8000 Series switch as a layer 2 (switching) or as a layer 3 (routing) device.

This guide provides information about using the features and capabilities of the CLI commands to perform layer 3 (routing) network management operations on Passport switches.

For general information about using the features and capabilities of the CLI commands to perform layer 2 (switching) operations, refer to *Reference for the Passport 8000 Series Command Line Interface Switching Operations*. For general information about networking features in Passport products, refer to *Networking Concepts for the Passport 8000 Series Switch*. For information about using the Passport Management Software Device Manager and VLAN Manager, refer to *Reference for the Passport 8000 Series Management Software Switching Operations* and *Reference for the Passport 8000 Series Management Software Routing Operations.*

Before You Begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies

Before using this guide, you must complete the following procedures. For a new switch:

- Install the switch (see the installation guide that came with your router).
- Connect the router to the network (see *Getting Started with the Passport 8600 Management Software)*.

Text Conventions

angle brackets < >	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: `ping <ip_address>`, you enter: `ping 192.32.10.12`
braces {}	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: `action <action choice>` the options for `<action choice>` are {none|flushMacFdb|flushArp|flushIp|flushAll |triggerRipUpdate}
brackets [ ]	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: `show log [tail]`, you can enter either: `show log` or `show log tail`.

italic text	Indicates file and directory names, new terms, and book titles.
`screen text`	Indicates commands and system output, for example, prompts and system messages. Example: `Passport-8600# show config verbose`
vertical line |	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: `config cli more <true|false>`, you must enter either: `config cli more true` or `config cli more false`, but not both.

Related Publications

For more information about using Passport Management Software or Passport switches, refer to the following publications:

- *Getting Started with the Passport 8600 Management Software* (part number 209663-B)

  Outlines the procedures for installing and booting your Passport switch, as well as instructions for installing the Passport Management Software.

- *Using the Passport 8600 Modules* (part number 207306-B)

  Provides information about Passport 8600 modules, including descriptions of their operational features, installation instructions, basic setup procedures, and technical specifications.

- *Installing the Passport 8010 Chassis* (part number 204518-B)

  Provides instructions in English and six other languages to install the Passport 8010 Chassis; includes technical specifications for the chassis.

- *Installing the Passport 8001PS AC Power Supply* (part number 204519-B)

  Provides instructions on installing the Passport 8001PS AC Power Supply; includes technical specifications for the power supply.

- *Reference for the Passport 8000 Series Management Software Switching Operations* (part number 207414-C)

  Describes how to use Device Manager to configure and manage layer 2 (switching) functions with the Passport switch, including procedures and illustrations of pertinent screens.

- *Reference for the Passport 8000 Series Command Line Interface Switching Operations* (part number 207308-C)

  Describes how to use the CLI to configure and manage layer 2 (switching) functions with the Passport switch, including procedures and illustrations of pertinent commands.

- *Reference for the Passport 8000 Series Management Software Routing Operations* (part number 207415-B)

  Describes how to use Device Manager to configure and manage layer 3 (routing) functions with the Passport switch, including procedures and illustrations of pertinent screens.

- *Networking Concepts for the Passport 8000 Series Switch* (part number 207307-C)

  General information and description of how the Passport 8000 Series switch handles various networking features such as VLANs, Multi-Link Trunking, OSPF, RIP, IPX, and so forth.

For more information about networking concepts, protocols, and topologies, you may want to consult the following sources:

- RFC 951 (BootP)
- RFC 1058 (RIP version 1)
- RFC 1723 (RIP version 2)
- RFC 1389 (RIP 2 Management Information Base (MIB))
- RFC 1213 (Network Management of TCP/IP MIB II)
- RFC 1493 (Bridge MIB)
- RFC 1573 (IANA If Type)
- RFC 1643 (Ether-like MIB)
- RFC 2131 (DHCP)
- RFC 2338 (VRRP)
- RFCs 1271 and 1757 (RMON)
- RFC 1850 (OSPF MIB)
- RFCs 1253, 1583 and 2178 (OSPF)
- RFCs 2474 and 2475 (DiffServ)
- RFCs 2597 and 2598 (DiffServ Per Hop Behavior)
- RFC 1112 (IGMP version 1)
- RFC 2236 (IGMP version 2)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- Enterprise MIB (located on the *Passport 8000 Series Software CD*)

You can print selected technical manuals and release notes free, directly from the Internet. Go to the *support.baynetworks.com/library/tpubs/* Web address. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web address at *www.adobe.com* to download a free copy of Acrobat Reader.

You can purchase Nortel Networks documentation sets, CDs, and selected technical publications at *www1.fatbrain.com/documentation/nortel*.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Billerica, MA	800-2LANWAN or (800) 252-6926
Santa Clara, CA	800-2LANWAN or (800) 252-6926
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5740-1700

Chapter 1
IP Routing and ARP Commands

This chapter describes the Run-Time CLI commands that are used to configure layer 3 (routing) functions in the Passport 8000 Series switch. The chapter includes sections about the following command groups used to configure routing characteristics:

- IP Routing Commands
- IP ARP Commands

IP Routing Commands

The general IP routing commands allow you to enable and disable IP forwarding (routing) on the switch, ports, and/or VLAN.

config ip Commands

The general `config ip` commands take the following syntax and format:

config ip followed by:	
`info`	Displays current default time-to-live characteristics (Figure 1-1).
`default-ttl <seconds>`	Sets the default time to live (ttl) value for a routed packet. It is the maximum number of seconds before a packet is discarded. • `<seconds>` is a number between 1 and 255. The default value of 255 is inserted in the ttl field whenever one is not supplied in the datagram header.

config ip followed by:	
forwarding disable	Disables IP forwarding (routing) on the entire switch. IP routing is disabled, allowing you to manage a Passport switch over a network without forcing the switch to also perform routing.
forwarding enable	Enables IP forwarding (routing) on the entire switch. Default is enable.
forwarding info	Displays whether IP forwarding is enabled or disabled.
mroute info	Displays IP multicast route settings.
mroute interface <ipaddr> info	Displays IP multicast routing interface information.
mroute interface <ipaddr> ttl <ttl>	Sets the default time-to-live for the multicast route interface.
route delete <ipaddr/mask>	Deletes a route. • <ipaddr/mask> is the IP address and mask for the route's destination.
route info	Displays route information.
route-discovery disable	Disables Internet Router Discovery Protocol (IRDP). This command will be fully implemented in a future release.
route-discovery enable	Enables IRDP. This command will be fully implemented in a future release.
route-discovery info	Displays whether route discovery is enabled or disabled.
static-route create <ipaddr/mask> next-hop <value> cost <value>	Adds a static or default route to the switch. • <ipaddr/mask> is the IP address and mask for the route's destination. • next-hop <value> is the IP address of the next hop router; the next router at which packets must arrive on this route. • cost <value> is the metric of the route.
static-route delete <ipaddr/mask> next-hop <value>	Deletes a static route. • <ipaddr/mask> is the IP address and mask for the route's destination. • next-hop <value> is the IP address of the next hop router; the next router packets must arrive at on this route.

config ip followed by:	
`static-route disable <ipaddr/mask> next-hop <value>`	Disables a static route. • `<ipaddr/mask>` is the IP address and mask for the route's destination. • `next-hop <value>` is the IP address of the next hop router; the next router at which packets must arrive on this route.
`static-route enable <ipaddr/mask> next-hop <value>`	Enables a static route. • `<ipaddr/mask>` is the IP address and mask for the route's destination. • `next-hop <value>` is the IP address of the next hop router; the next router at which packets must arrive on this route.
`static-route info`	Displays characteristics of the created static route.

Figure 1-1 shows `config ip info` output.

```
Passport-8610/config/ip# info

Sub-Context: arp dhcp-relay dvmrp forwarding l3-igmp mroute ospf
policy rip route route-discovery static-route traffic-filter udpfwd
Current Context:

                default-ttl : 255
```

Figure 1-1. *config ip info* Command Output

Figure 1-2 shows `config ip static-route info` command output.

```
Passport-8610# config ip static-route info

                    create :
                                    - 0.0.0.0/0.0.0.0
                            next-hop - 10.10.40.1
                                cost - 1
                              status - ACTIVE
                              enable - TRUE

                   disable : N/A
                    delete : N/A
                    enable : N/A
```

Figure 1-2. *config ip static-route info* Command Output

show ip Commands

These commands display the general IP characteristics of the switch.

show ip forwarding Command

The `show ip forwarding` command displays the status of IP forwarding (routing) on the switch. Figure 1-3 is a sample display.

```
Passport-8610# show ip forwarding

IP Forwarding is enabled
IP Default TTL is 255 seconds
IP ARP life time is 360 seconds
```

Figure 1-3. *show ip forwarding* Command Output

show ip interface Command

The `show ip interface` command displays the IP interfaces on the switch.

Figure 1-4 is a sample display.

```
Passport-8610# show ip interface

================================================================================
                                     Ip Interface
================================================================================
INTERFACE IP             NET            BCASTADDR  REASM    VLAN  BROUTER
          ADDRESS        MASK           FORMAT     MAXSIZE  ID    PORT
--------------------------------------------------------------------------------
Port9/1   1.2.3.4        255.0.0.0      ones       1500     1000  true
Port9/13  5.5.5.5        255.0.0.0      ones       1500     5     true
```

Figure 1-4. *show ip interface* Command Output

show ip route-discovery Command

The `show ip route-discovery` command shows whether or not route discovery is enabled on the device.

show ip route info Command

The `show ip route info` command displays the existing IP route table for the switch or for a specific net or subnet.

This command uses the syntax:

```
show ip route info [<ip address>][-s <value>]
```

where:

`[<ip address>]` is the specific net (1.2. = 1.2.0.0) {a.b.c.d}.

`[-s <value>]` is the specific subnet {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.

Figure 1-5 is an example.

```
Passport-8610# show ip route info

================================================================================
                                    Ip Route
================================================================================
            DST             MASK            NEXT COST VLAN   PORT  OWNER
--------------------------------------------------------------------------------
       31.0.0.0        255.0.0.0        31.1.1.1    1 2194   -/-   LOCAL
       50.0.0.0        255.0.0.0       130.1.1.2  220 2221   3/30   OSPF
      120.0.0.0        255.0.0.0       130.1.1.2  210 2221   3/30   OSPF
      130.1.0.0      255.255.0.0       130.1.1.1    1 2221   -/-   LOCAL
      200.1.1.0    255.255.255.0       130.1.1.2  210 2221   3/30   OSPF
Total 5
```

Figure 1-5. *show ip route info* Command Output

show ip static-route info Command

The `show ip static-route info` command displays the existing IP static routes for the switch or for a specific net or subnet.

This command uses the syntax:

```
show ip static-route info [<ip address>][-s <value>]
```

where:

`[<ip address>]` is the specific net (1.2. = 1.2.0.0) {a.b.c.d}.

`[-s <value>]` is the specific subnet {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.

Figure 1-6 is an example.

```
Passport-8610# show ip static-route info

================================================================================
                                    Ip Static Route
================================================================================
           DEST            MASK            NEXT  COST PREFERENCE   STATUS ENABLE
--------------------------------------------------------------------------------
        0.0.0.0         0.0.0.0      10.10.40.1     1          0   ACTIVE   TRUE
Total 1
```

Figure 1-6. *show ip static-route info* Command Output

config ethernet <ports> ip Commands

These commands are the more generic port-related IP routing commands. Other port commands are included in the section dealing with the protocol or feature (for example, DHCP).

In order for the `config ethernet <ports> ip` commands to take effect, IP forwarding must be enabled on the switch; by default on the Passport 8000 Series switch, forwarding is enabled.

The command uses the syntax:

```
config ip forwarding enable
```

The port commands require the parameter `<ports>` as the port or list of ports on which you are running the command {slot/port[-slot/port][, ...]}.

These commands take the following syntax and parameters:

config ethernet <ports> ip followed by:	
info	Displays configured IP characteristics on the port.
create <ipaddr/mask> <vid> [mac_offset <value>]	Assigns an IP address to a port. Assigning an IP address to a port creates a Brouter port (see page 1-8). • <ipaddr/mask> is the IP address and mask {a.b.c.d}. • <vid> is the VLAN ID {1..4094}. • [mac_offset <value>] is a user-assigned MAC address. This MAC address is in place of the default MAC address.
delete <ipaddr>	Deletes an IP address from a Brouter port.

Figure 1-7 is a sample of the config ethernet ip info command.

```
Passport-8610# config ethernet 9/13 ip info

Sub-Context:
Current Context:

Port 9/13 :
                     create : 5.5.5.5/255.0.0.0 Vlan5 mac_offset 0
                     delete : N/A
```

Figure 1-7. *config ethernet ip info* Command Output

show ports info ip Command

The `show ports info ip` command displays routing (IP) information about the specified port or for all ports.

This command uses the syntax:

```
show ports info ip [<ports>]
```

Figure 1-8 is a sample display.

```
Passport-8610# show ports info ip

================================================================================
                                     Port Ip
================================================================================
PORT     IP_ADDRESS       NET_MASK         BROADCAST  REASM   ADVERTISE
NUM                                                   MAXSIZE WHEN_DOWN
--------------------------------------------------------------------------------
9/13     5.5.5.5          255.0.0.0        ones       1500    disable
```

Figure 1-8. *show ports info ip* Command Output

Brouter Ports

To create a brouter port, configure a routed IP policy-based single-port VLAN. You create a brouter port by assigning an IP address to a port and specifying a VLAN ID for that port. Use the following command:

```
config ethernet <ports> ip create <ipaddr/mask> <vid>
```

show ports info brouter-port Command

The `show ports info brouter-port` command displays brouter port information for their associated VLANs.

This command uses the syntax:

```
show ports info brouter-port
```

Figure 1-9 is an example.

```
Passport-8610# show ports info brouter-port

        Port       Vlan Id
        ====       =======
        1/1           2
```

Figure 1-9. *show ports info brouter-port* Command Output

vlan ip Commands

These commands are the general routing commands on the VLAN. Other VLAN commands are included in the section dealing with the protocol or feature (for example, DHCP).

config vlan ip Commands

The general `config vlan ip` commands require a VLAN ID `<vid>` from 1 to 4094.

The commands take the following syntax and parameters:

config vlan <vid> ip followed by:	
`info`	Displays VLAN routing characteristics.
`create <ipaddr/mask> [mac_offset <value>]`	Assigns an IP address and subnet mask to the VLAN. • `<ipaddr/mask>` is the IP address and mask {a.b.c.d}. • `[mac_offset <value>]` is a user-assigned MAC address. This MAC address is in place of the default MAC address.
`delete <ipaddr>`	Deletes the specified VLAN address.

Figure 1-10 shows an example of the `config vlan ip info` command.

```
Passport-8610# config vlan 5 ip info

Sub-Context:
Current Context:

                     create : 5.5.5.5/255.0.0.0 mac_offset 0
                     delete : N/A
```

Figure 1-10. *config vlan ip info* Command Output

show vlan info ip Command

The `show vlan info ip` command displays the routing (IP) configuration for all VLANs on the switch or for the specified VLAN.

This command uses the syntax:

```
show vlan info ip [<vid>]
```

Figure 1-11 is a sample display.

```
Passport-8610# show vlan info ip

================================================================================
                                     Vlan Ip
================================================================================
VLAN IP              NET              BCASTADDR REASM    ADVERTISE
ID   ADDRESS         MASK             FORMAT    MAXSIZE  WHEN_DOWN
--------------------------------------------------------------------------------
1    10.10.40.3      255.255.255.0    ones      1500     disable
```

Figure 1-11. *show vlan info ip* Command Output

IP ARP Commands

The Address Resolution Protocol (ARP) commands enable you to add and delete static entries in the ARP table and to display the ARP table. The ARP table maps MAC addresses to IP addresses. If you add an ARP entry for a VLAN, the VLAN is associated with the MAC address you specify. When you display the ARP table, all entries (static and dynamic) are displayed. Before you can add an ARP entry to a port or port-based VLAN, an IP address must already be assigned to the port or VLAN and routing must already be enabled.

config ip arp Commands

The `config ip arp` commands configure ARP on the switch.

The commands take the following syntax and parameters:

config ip arp followed by:	
`info`	Displays ARP characteristics.
`add ports <value> ip <value> mac <value> [vlan <value>]`	Adds a static entry to the ARP table. • `ports <value>` are the port numbers, shown as slot/port. • `ip <value>` is the IP address {a.b.c.d}. • `mac <value>` is the 48-bit hardware MAC address in the format {0x00:0x00:0x00:0x00:0x00:0x00}. • `vlan <value>` is the name or number of a VLAN.
`aging <minutes>`	Sets the length of time in seconds an entry remains in the ARP table before timeout. • `<minutes>` is a number between 1 and 32767.
`delete <ipaddr>`	Removes an entry from the ARP table. • `<ipaddr>` is the IP address {a.b.c.d}.

Figure 1-12 shows a sample of the `config ip arp info` command.

```
Passport-8610# config ip arp info

Sub-Context:
Current Context:

                        aging : 360
                       delete : N/A
                          add :

                                  ports - 1/30
                                     ip - 10.10.40.142
                                    mac - 00:e0:16:68:8c:00
                                   vlan - 1

                                  ports - 1/2
                                     ip - 10.10.40.194
                                    mac - 00:e0:16:7f:16:00
                                   vlan - 1
```

Figure 1-12. *config ip arp info* Command (Partial Output)

show ip arp info Command

The `show ip arp info` command displays the ARP table.

The command uses the format:

```
show ip arp info [<ip address>] [-s <value>]
```

where:

`[<ip address>]` is the specific net IP address for the table .

`[-s <value>]` is the specific subnet in the format (a.b.c.d/x|a.b.c.d/x.x.x.x|default).

An example of the output from this command with no IP address or subnet specified is shown in Figure 1-13. In the TTL column, the output is measured in seconds.

```
Passport-8610# show ip arp info

================================================================================
                                      Ip Arp
================================================================================
  IP_ADDRESS       MAC_ADDRESS      VLAN  PORT    TYPE    TTL
--------------------------------------------------------------------------------
161.69.150.10   00:e0:16:ff:01:3a  2       1/1   DYNAMIC 2133
161.69.150.1    00:80:2d:23:02:00  2        -    LOCAL   2160
161.69.150.255  ff:ff:ff:ff:ff:ff  2       1/1   LOCAL   2160
161.69.100.255  ff:ff:ff:ff:ff:ff  2       1/1   LOCAL   2160
Total 4
```

Figure 1-13. *show ip arp info* Command Output

config ethernet <ports> ip arp Commands

These commands allow you to configure IP ARP on specific ports. The commands require the parameter `<ports>` as the port or list of ports on which you are running the command {slot/port[-slot/port][, ...]}.

config ethernet <ports> ip Commands

The `config ethernet <ports> ip` commands take the following syntax and parameters:

config ethernet <ports> ip followed by:	
`arp-response disable`	Disables ARP responses on the port.
`arp-response enable`	Enables ARP responses on the port.
`arp-response info`	Displays ARP response status on the port.
`proxy disable`	Disables proxy ARP on the port.
`proxy enable`	Enables proxy ARP on the port, allowing a router to answer a local ARP request for a remote destination.
`proxy info`	Displays ARP proxy status on the port.

Figure 1-14 shows a sample of the `config ethernet <ports> ip arp-response info` command.

```
Passport-8610# config ethernet 9/2 ip arp-response info

Sub-Context:
Current Context:

Port 9/2 :
                arp-response : enable
```

Figure 1-14. *config ethernet ip arp-response info* Command Output

show ports info arp Command

The `show ports info arp` command displays ARP information about the specified port or for all ports.

The command uses the syntax:

```
show ports info arp [<ports>]
```

Figure 1-15 is a sample display.

```
Passport-8610# show ports info arp

================================================================================
                                        Port Arp
================================================================================
PORT_NUM DOPROXY    DORESP
--------------------------------------------------------------------------------
9/1      false      true
9/2      false      true
9/3      false      true
9/4      false      true
9/5      false      true
9/6      false      true
9/7      false      true
9/8      false      true
9/9      false      true
9/10     false      true
```

Figure 1-15. *show ports info arp* Command (Partial Output)

config vlan ip arp Commands

The general commands for VLAN ARP require a VLAN ID `<vid>` from 1 to 4094.

config vlan ip arp Command

The `config vlan ip arp` commands allow you to configure IP ARPs on VLANs.

The commands take the following syntax and parameters:

config vlan <vid> ip followed by:	
`arp-response disable`	Disables ARP response on the VLAN.
`arp-response enable`	Enables ARP response on the VLAN. This state is the default state.
`arp-response info`	Displays VLAN ARP response status.
`proxy disable`	Disables proxy ARP on the VLAN. This is the default state.
`proxy enable`	Enables proxy ARP on the VLAN.
`proxy info`	Displays proxy ARP status on the VLAN.

Figure 1-16 shows a sample of the `config vlan ip proxy info` command.

```
Passport-8610# config vlan 1 ip proxy info

Sub-Context:
Current Context:

                        proxy : disable
```

Figure 1-16. *config vlan ip proxy info* Command Output

show vlan info arp Command

The `show vlan info arp` command displays the ARP configuration for all VLANs or the specified VLAN.

The command uses the syntax:

```
show vlan info arp [<vid>]
```

A sample output is shown in Figure 1-17.

```
Passport-8610# show vlan info arp

================================================================================
                                        Vlan Arp
================================================================================
VLAN ID  DOPROXY    DORESP
--------------------------------------------------------------------------------
1        false      true
2        false      true
3        false      true
4        false      true
```

Figure 1-17. *show vlan info arp* Command Output

Chapter 2
DHCP and UDP Commands

This chapter describes the Run-Time CLI commands that are used to configure DHCP and UDP functions in the Passport 8000 Series switch. The chapter includes sections about the following command groups used to configure routing characteristics:

- DHCP Relay Commands
- UDP Commands

DHCP Relay Commands

Dynamic Host Configuration Protocol (DHCP), an extension of the Bootstrap Protocol (BootP), is used to dynamically provide host configuration information to the workstations. Use the port DHCP relay commands to set DHCP relay behavior on a port and the VLAN DHCP commands to set DHCP relay behavior on a VLAN.

DHCP relay must be enabled on the path for port or VLAN configuration to take effect.

config ip dhcp-relay Commands

The `config ip dhcp-relay` commands allow you to view and configure DHCP parameters globally.

The `config ip dhcp-relay` commands use the following syntax and parameters:

config ip dhcp-relay followed by:	
`info`	Displays current DHCP global configuration on the switch.
`create-fwd-path agent <value> server <value> [mode <value>] [state <value>]`	Configures the forwarding path from the client to the server. • `agent <value>` is the IP address configured on an interface (a locally configured IP address). • `server <value>` is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out the interface. • `[mode <value>]` is to forward BootP messages only, DHCP messages only, or both {bootp|dhcp|bootp_dhcp}. • `[state <value>]` enables or disables the forwarding path.
`enable-fwd-path agent <value> server <value>`	Enables DHCP relaying on the path from the IP address to the server. • `agent <value>` is the IP address configured on an interface (a locally configured IP address). • `server <value>` is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out the interface.
`delete-fwd-path agent <value> server <value>`	Deletes the forwarding path from the client to the server. • `agent <value>` is the IP address configured on an interface (a locally configured IP address). • `server <value>` is the IP address of the DHCP server in the network.

config ip dhcp-relay followed by:	
`disable-fwd-path agent <value> server <value>`	Disables DHCP relaying on the path from the IP address to the server. This is the default. • `agent <value>` is the IP address configured on an interface (a locally configured IP address). • `server <value>` is the IP address of the DHCP server in the network.
`mode <mode> agent <value> server <value>`	Modifies DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both. • `<mode>` is {bootp|dhcp|bootp_dhcp}. • `agent <value>` is the IP address configured on an interface (a locally configured IP address). • `server <value>` is the IP address of the DHCP server in the network.

show ip dhcp-relay Commands

show ip dhcp-relay fwd-path Command

The `show ip dhcp-relay fwd-path` command displays DHCP routing information, including interface, server, enabled or disabled, and mode (forward BootP messages only, DHCP messages only, or both).

show ip dhcp-relay counters Command

The `show ip dhcp-relay counters` command displays DHCP counter information, including the number of requests and the number of replies for each interface.

Figure 2-1 shows an example of `show ip dhcp-relay counters` command.

```
Passport-8610/show/ip/dhcp-relay# counters

================================================================================
                                      Dchp
================================================================================
INTERFACE       REQUESTS  REPLIES
--------------------------------------------------------------------------------
10.10.40.1      0         0
```

Figure 2-1. *show ip dhcp-relay counters* Command Output

config ethernet <ports> ip dhcp-relay Commands

The `config ethernet ip dhcp-relay` commands allow you to view and configure DHCP parameters on the specified port(s).The port commands require the parameter `<ports>` as the port or list of ports on which you are running the command {slot/port[-slot/port][, ...]}.

The commands use the following syntax and parameters:

config ethernet <ports> ip dhcp-relay followed by:	
`info`	Displays current DHCP configuration on the port.
`broadcast <enable|disable>`	Sets whether or not the server reply is sent as a broadcast or unicast back to the end station.
`disable`	Disables DHCP relaying on the port.This is the default state.
`enable`	Enables DHCP relaying on the port.
`max-hop <max-hop>`	Sets the maximum number of hops before a BootP/DHCP packet is discarded (1 to 16). The default is 4.
`min-sec <min-sec>`	Sets the minimum seconds count set for DHCP. If the “secs” field in the BootP/DHCP packet header is greater than this value, the switch relays or forwards the packet; otherwise, the packet is dropped (0 to 65535). The default is 0 seconds.
`mode <mode>`	Sets DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

Figure 2-2 shows a sample of the `config ethernet ip dhcp-relay info` command.

```
Passport-8610# config ethernet 9/2 ip dhcp-relay info

Sub-Context:
Current Context:

Port 9/2 :
                  dhcp-relay : enable
                   broadcast : disable
                     max-hop : 4
                     min-sec : 0
                        mode : both
```

Figure 2-2. *config ethernet ip dhcp-relay info* Command Output

show ports dhcp-relay Commands

These commands display information about DHCP on the port.

show ports info dhcp-relay Command

The `show ports info dhcp-relay` command displays the DHCP parameters for a specified port or all ports.

The command uses the format:

```
show ports info dhcp-relay [<ports>]
```

Figure 2-3 is a sample display.

```
Passport-8610# show ports info dhcp-relay

================================================================================
                                      Port Dhcp
================================================================================
PORT_NUM ENABLE   MAX_HOP  MIN_SEC  MODE  ALWAYS_BROADCAST
--------------------------------------------------------------------------------
9/1      false    4        0        both  false
9/2      true     4        0        both  false
9/3      false    4        0        both  false
9/4      false    4        0        both  false
9/5      false    4        0        both  false
9/6      false    4        0        both  false
9/7      false    4        0        both  false
```

Figure 2-3. *show ports info dhcp-relay* Command (Partial Output)

show ports stats dhcp-relay Command

The `show ports stats dhcp-relay` command displays DHCP statistics for a specified port or for all ports.

The command uses the syntax:

```
show ports stats dhcp-relay [<ports>]
```

Figure 2-4 is a sample display.

```
Passport-8610# show ports stats dhcp-relay

=========================================================================
                                        Port Stats Dhcp
=========================================================================
PORT_NUM NUMREQUEST NUMREPLY
-------------------------------------------------------------------------
1/1      0          0
3/1      0          0
3/2      0          0
3/3      0          0
3/4      0          0
3/5      0          0
```

Figure 2-4. *show ports stats dhcp-relay* Command (Partial Output)

config vlan <vid> ip dhcp-relay Commands

The `config vlan <vid> ip dhcp-relay` commands allow you to configure DHCP routing on the VLAN. The commands require a VLAN ID `<vid>` from 1 to 4094.

The commands use the following syntax and parameters:

config vlan <vid> ip dhcp-relay followed by:	
`info`	Displays DHCP characteristics on the VLAN.
`broadcast <enable|disable>`	Sets whether or not the server reply is sent as a broadcast back to the end station.
`disable`	Disables DHCP relaying on the VLAN. This is the default state.
`enable`	Enables DHCP relaying on the VLAN.
`max-hop <max-hop>`	Sets the maximum number of hops before the BootP/DHCP packet is dropped (1 to 16).
`min-sec <min-sec>`	Sets the minimum seconds count for DHCP. If the secs field in the packet header is greater than this value, the switch forwards the packet; otherwise it is dropped (0 to 65535).
`mode <mode>`	Sets DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.

Figure 2-5 shows a sample of the `config vlan ip dhcp-relay info` command.

```
Passport-8610# config vlan 1 ip dhcp-relay info

Sub-Context:
Current Context:

                  dhcp-relay : disable
                   broadcast : disable
                     max-hop : 4
                     min-sec : 0
                        mode : both
```

Figure 2-5. *config vlan ip dhcp-relay info* Command Output

show vlan info dhcp-relay Command

The `show vlan info dhcp-relay` command displays the DHCP parameters for all VLANs or for the specified VLAN. The interface index (IF Index) is assigned as the VLAN is created. Numbers 1 to 256 are ports; numbers above 257 are VLANs.

This command uses the syntax:

```
show vlan info dhcp-relay [<vid>]
```

Figure 2-6 is a sample.

```
Passport-8610# show vlan info dhcp-relay

=========================================================================
                                          Vlan Dhcp
=========================================================================
VLAN IF            MAX    MIN            ALWAYS
ID   INDEX  ENABLE HOP    SEC    MODE    BCAST
-------------------------------------------------------------------------
1    2049   false  4      0      both    false
2    2050   false  4      0      both    false
```

Figure 2-6. *show vlan info dhcp-relay* Command Output

UDP Commands

Some network applications, such as the NetBIOS name service, rely on a User Data Protocol (UDP) broadcast to request a service or to locate a service. By default, broadcasts are not forwarded by a router. UDP broadcast forwarding is a generalized mechanism for the router to selectively forward UDP broadcasts.

The basic procedure for setting up UDP broadcast forwarding is:

- Use the `config ip udpfwd protocol` commands to enter protocols in a protocol table.
- Use the `config ip udpfwd portfwdlist` commands to create and name the port forward list and assign protocols and servers to the port forward list.
- Use the `config ip interface` commands to apply the port forward list to the appropriate interfaces.

The `config ip udpfwd info` command displays the current UDP forwarding configuration.

config ip udpfwd protocol Commands

The UDP forwarding protocol commands require the `<udpport>` parameter as the UDP protocol port number {1..65535}.

The commands use the following syntax:

config ip udpfwd protocol <udpport> followed by:	
`create <protoname>`	Creates a new UDP protocol. • `<protoname>` is the UDP protocol name {string}.
`delete`	Deletes a UDP port protocol.
`info`	Displays created and/or deleted UDP protocols.

config ip udpfwd portfwdlist Commands

The UDP forwarding port forward list commands require the `<fwdlistid>` parameter as the port forwarding list number {1..1000}.

The commands use the following syntax and parameters:

config ip udpfwd portfwdlist <fwdlistid> followed by:	
`info`	Displays the current configuration for the port forward list ID.
`add-portfwd <udpport> <ipaddr>`	Adds a UDP protocol port to the specified port forwarding list. • `<udpport>` is a UDP protocol port {1..65535}. • `<ipaddr>` is an IP address.
`create`	Creates a UDP port forwarding list.
`delete`	Deletes a port forward list ID.
`name <name>`	Assigns a name to the UDP port forwarding list. • `<name>` is {string}.
`remove-portfwd <udpport> <ipaddr>`	Removes a protocol port forwarding entry and IP address from the list. • `<udpport>` is a UDP protocol port {1..65535}. • `<ipaddr>` is an IP address.

config ip udpfwd interface Commands

The UDP forwarding interface commands require an IP address `<ipaddr>` and use the following syntax and parameters:

config ip udpfwd interface <ipaddr> followed by:	
`info`	Displays the current configuration of the UDP interface.
`create <fwdlistid>`	Assigns a forwarding list ID {1..1000} to an interface IP address.
`delete`	Removes the forwarding list from the IP address.

config ip udpfwd interface <ipaddr> followed by:	
maxttl <maxttl>	Sets maximum time-to-live for the UDP broadcast forwarded by the interface.
udpportfwdlist <fwdlistid>	Changes the port forwarding list {1..1000}.

show ip udpfwd Commands

These commands display information about the UDP forwarding characteristics of the switch.

show ip udpfwd interface info Command

The `show ip udpfwd interface info` command displays information about the UDP interface for all IP addresses or a specified IP address.

The command uses the syntax:

```
show ip udpfwd interface info [<ipaddr>]
```

Figure 2-7 is a sample display.

```
Passport-8610/show/ip/udpfwd/interface# info

================================================================================
                                    Udp Broadcast Interface Forwarding Tbl
================================================================================
INTF_ADDR       FWD    MAXTTL RXPKTS  FWDPKTS DRPTTLEX DRPDEST  DRP_UNKNOWN
                LISTID                                 UNREACH  PROTOCOL
--------------------------------------------------------------------------------
161.69.150.1    1      4      9       7       0        0        0
```

Figure 2-7. *show ip udpfwd interface info* Command Output

show ip udpfwd portfwd info Command

The `show ip udpfwd portfwd info` command displays the UDP port forwarding table.

The command uses the syntax:

```
show ip udpfwd portfwd info
```

Figure 2-8 is a sample.

```
Passport-8610/show/ip/udpfwd/portfwd# info

================================================================================
                                      Udp Prot Fwd Tbl
================================================================================
UDP_PORT FORWARDING_ADDR FWDPKTS  DRPTTLEX DRPDEST_UNKNOWN
--------------------------------------------------------------------------------
1        1.1.1.1         7        0        0
1        2.2.2.2         0        0        0
```

Figure 2-8. *show ip udpfwd portfwd info* Command Output

show ip udpfwd portfwdlist info Command

The `show ip udpfwd portfwdlist info` command displays the UDP Port Forwarding List Table for the specified list or all lists on the switch.

The command uses the syntax:

```
show ip udpfwd portfwdlist info [<fwdlistid>]
```

show ip udpfwd protocol info Command

The `show ip udpfwd protocol info` command displays the UDP protocol table with the UDP port numbers for each supported or designated protocol.

The command uses the syntax:

```
show ip udpfwd protocol info
```

Figure 2-9 is an example.

```
Passport-8610/show/ip/udpfwd/protocol# info

================================================================================
                                        Udp Protocol Tbl
================================================================================
UDP_PORT PROTOCOL_NAME
--------------------------------------------------------------------------------
1        NewPIOne
37       Time Service
49       TACACS Service
53       DNS
69       TFTP
137      NetBIOS NameSrv
138      NetBIOS DataSrv
1024     UserDefinedLab Prot
```

Figure 2-9. *show ip udpfwd protocol info* Command Output

Chapter 3
RIP and OSPF Commands

This chapter describes the Run-Time CLI commands that are used to configure RIP and OSPF layer 3 (routing) functions in the Passport 8000 Series switch. The chapter includes sections about the following command groups used to configure routing characteristics:

- RIP Commands
- OSPF Commands

RIP Commands

This section describes the commands used to configure Routing Information Protocol (RIP) on the Passport 8000 Series switch. You configure RIP on a port or on a VLAN, but you must enable it globally first.

config ip rip Commands

The `config ip rip` commands allow you to enable or disable RIP globally on the switch.

These commands are as follows:

config ip rip followed by:	
info	Displays current RIP configuration settings.
disable	Globally disables RIP on the switch.
domain <ipaddr> <value>	Changes the RIP interface configuration domain, the value inserted into the routing domain field of all RIP packets sent on this interface. • <ipaddr> is the interface IP address {a.b.c.d}. • <value> is the domain value {0 to 39321}.
enable	Globally enables RIP on the switch.
holddown <seconds>	Sets the RIP holddown timer value, the length of time (in seconds) that RIP will continue to advertise a network after determining that it is unreachable. • <seconds> is 0 to 360, with a default of 120.
updatetime <seconds>	Sets RIP update timer, the time interval between RIP updates. • <seconds> is 0 to 360, with a default of 30 seconds.

receive <ipaddr> mode <value>	Changes the RIP interface receive configuration.
	• <ipaddr> is the IP address of the interface.
	• mode <value> indicates what RIP versions to accept:
	  • rip1 = RIP version 1.
	  • rip2 = RIP version 2.
	  • rip1orrip2= receive in either RIP 1 or 2.

send <ipaddr> mode <value>	Changes the RIP interface send configuration.
	• <ipaddr> is the IP address of the interface.
	• mode <value> indicates what RIP versions to send:
	  • notsend = do not send
	  • rip1 = RIP version 1.
	  • rip2 = RIP version 2.
	  • rip1Compatible= receive in either RIP 1 or 2.

Figure 3-1 shows a sample of the `config ip rip info` command.

```
Passport-8610# config ip rip info

Sub-Context:
Current Context:

                     enable : false
                   holddown : 120
                 updatetime : 30
                     domain :
                                      - 10.10.40.34
                                      - 0
                    receive :
                                      - 10.10.40.34
                                 mode - rip1OrRip2
                       send :
                                      - 10.10.40.34
                                 mode - rip1Compatible
```

Figure 3-1. *config ip rip info* Command Output

show ip rip Commands

These commands display information about the RIP configuration on the switch.

show ip rip info Command

The `show ip rip info` command displays the RIP global status on the switch.

The command's syntax is:

```
show ip rip info
```

Figure 3-2 is a sample.

```
Passport-8610/show/ip/rip# info

================================================================================
                                        Rip Global
================================================================================
           Rip : Disabled
   Update Time : 30
 HoldDown Time : 120
 Route Changes : 0
       Queries : 0
        Domain : 0
```

Figure 3-2. *show ip rip* Command Output

show ip rip interface Command

The `show ip rip interface` command displays information about the specified RIP interface or all RIP interfaces on the switch.

The command uses the syntax:

```
show ip rip interface [<ipaddr>]
```

Figure 3-3 is a sample display.

```
Passport-8610# show ip rip interface

================================================================================
                                    Rip Interface
================================================================================
IP_ADDR         RIP_ENABLE      SEND                 RECEIVE
--------------------------------------------------------------------------------
5.5.5.5         false           rip1Compatible      rip1OrRip2
```

Figure 3-3. *show ip rip interface* Command Output

config ethernet <ports> ip rip Commands

The `config ethernet <ports> ip rip` commands configure RIP on specified ports. RIP must also be enabled globally for the commands to take effect. These commands use the `<ports>` parameter to specify the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.

The port-based RIP commands have the following syntax and parameters:

config ethernet <ports> ip rip followed by:	
`info`	Displays RIP characteristics on the port.
`advertise-when-down <enable|disable>`	If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. **Note**: When you configure a port without any link and enable advertise-when-down, it will not advertise your route until the port is active. Then the route will be advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.

config ethernet <ports> ip rip followed by:	
auto-aggr <enable|disable>	Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disable.
default-listen <enable|disable>	Enables or disables RIP listen to accept the default route via RIP.
default-supply <enable|disable>	Enables or disables an advertisement of a default route only if one exists in the routing table.
disable	Disables RIP on the port. This setting is the default.
enable	Enables RIP on the port.
listen <enable|disable>	Configures whether or not the switch will listen for a default route without listening for all routes.
manualtrigger	Allows you to manually issue a RIP update.
poison <enable|disable>	Sets whether or not RIP routes on the port learned from a neighbor are advertised back to the neighbor. If disabled, split horizon is invoked and IP routes learned from an immediate neighbor are not advertised back to the neighbor. If enabled, the RIP updates sent to a neighbor from which a route is learned are “poisoned” with a metric of 16. Therefore, the receiver neighbor will ignore this route because the metric 16 indicates infinite hops in the network.
supply <enable|disable>	Enables or disables the switch to supply RIP routes with including the default routes.
trigger <enable|disable>	Enables or disables automatic triggered updates for RIP.

Figure 3-4 shows a sample of the `config ethernet ip rip info` command.

```
Passport-8610# config ethernet 9/2 ip rip info

Sub-Context:
Current Context:

Port 9/2 :
         advertise-when-down : disable
                   auto-aggr : disable
              default-listen : enable
              default-supply : disable
                         rip : disable
                     trigger : disable
                      listen : enable
               manualtrigger : N/A
                      poison : disable
                      supply : enable
```

Figure 3-4. *config ethernet ip rip info* Command Output

Table 3-1 indicates the relationship between switch action and the RIP supply and listen settings.

Table 3-1. RIP Supply and Listen Settings and Switch Action

RIP Supply Settings		RIP Listen Settings		Switch Action
Supply	**Default Supply**	**Listen**	**Default Listen**	
Disabled	Disabled			Sends no RIP updates.
Enabled	Disabled			Sends RIP updates except the default.
Disabled	Enabled			Sends only the default (default route must exist in routing table).
Enabled	Enabled			Sends RIP updates including the default route (if it exists).
		Disabled	Disabled	Does not listen for RIP updates.
		Enabled	Disabled	Listens for all RIP updates except the default.

Table 3-1. RIP Supply and Listen Settings and Switch Action

RIP Supply Settings		RIP Listen Settings		Switch Action
Supply	**Default Supply**	**Listen**	**Default Listen**	
		Disabled	Enabled	Listens only for the default.
		Enabled	Enabled	Listens for RIP updates including the default route (if it exists).

show ports info rip Command

The `show ports info rip` command displays information about the RIP parameters of the specified port or all ports.

The command uses the format:

```
show ports info rip [<ports>]
```

Figure 3-5 is an example.

```
Passport-8610# show ports info rip

================================================================================
                                      Port Rip
================================================================================
PORT         ADVERTISE ACCEPT  TRIGGERED AUTOAGG
NUM   ENABLE DEFAULT   DEFAULT UPDATE    ENABLE  SUPPLY LISTEN POISON
--------------------------------------------------------------------------------
9/1   false  false     false   false     false   true   true   false
9/2   false  false     true    false     false   true   true   false
9/3   true   false     false   false     false   true   true   false
9/4   false  false     false   false     false   true   true   false
9/5   false  false     false   false     false   true   true   false
9/6   false  false     false   false     false   true   true   false
9/7   false  false     false   false     false   true   true   false
```

Figure 3-5. *show ports info rip* Command (Partial Output)

config vlan <vid> ip rip Commands

The `config vlan <vid> ip rip` commands allow you to set RIP parameters for a VLAN, where `<vid>` is the VLAN ID (1 to 4094).

These commands have the following syntax and parameters:

config vlan <vid> ip rip followed by:	
`info`	Displays RIP characteristics on the VLAN.
`advertise-when-down <enable|disable>`	If enabled, the network on this interface will be advertised as up, even if the port is down. The default is disabled. **Note**: When you configure a port without any link and enable advertise-when-down, it will not advertise your route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.
`auto-aggr <enable|disable>`	Enables or disables automatic route aggregation on the VLAN. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disable.
`default-listen <enable|disable>`	Allows the user to enable or disable setting RIP listen to accept the default route via RIP.
`default-supply <enable|disable>`	Allows the user to send a default route only if one exists in the routing table.
`disable`	Disables RIP on the VLAN. This is the default setting.
`enable`	Enables RIP on the VLAN.
`listen <enable|disable>`	Configures whether or not the switch will listen for RIP routes.
`manualtrigger`	Allows you to manually issue RIP updates.

config vlan <vid> ip rip followed by:	
poison <enable|disable>	Sets whether or not RIP routes on the VLAN learned from a neighbor are advertised back to the neighbor. If disabled, split horizon is invoked and IP routes learned from an immediate neighbor are not advertised back to the neighbor. If enabled, the RIP updates sent to a neighbor from which a route is learned are “poisoned” with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network.
supply <enable|disable>	Enables or disables the switch to supply RIP updates.
trigger <enable|disable>	Enables or disables automatic triggered updates for RIP.

Refer to Table 3-1 on page 3-6 for actions resulting from RIP supply and listen settings.

Figure 3-6 shows a sample of the `config vlan ip rip info` command.

```
Passport-8610# config vlan 1 ip rip info

Sub-Context:
Current Context:

         advertise-when-down : disable
                   auto-aggr : disable
              default-listen : disable
              default-supply : disable
                         rip : disable
                     trigger : disable
                      listen : enable
               manualtrigger : N/A
                      poison : disable
                      supply : enable
```

Figure 3-6. *config vlan ip rip info* Command Output

show vlan info rip Command

The `show vlan info rip` command shows the RIP parameters for all VLANs or for the specified VLAN.

The command uses the format:

```
show vlan info rip [<vid>]
```

Figure 3-7 is an example.

```
Passport-8610# show vlan info rip

================================================================================
                                    Vlan Rip
================================================================================
VLAN        ADVERTISE ACCEPT  TRIGGERED AUTOAGG
ID   ENABLE DEFAULT   DEFAULT UPDATE    ENABLE  SUPPLY LISTEN POISON
--------------------------------------------------------------------------------
1    false  false     false   false     false   true   true   false
2    false  false     false   false     false   true   true   false
3    false  false     false   false     false   true   true   false
4    false  false     false   false     false   true   true   false
```

Figure 3-7. *show vlan info rip* Command Output

OSPF Commands

Routers use the Open Shortest Path First (OSPF) protocol to exchange network topology information among themselves, providing each router with a map of the network.

config ip ospf Commands

The following command groups are used to configure OSPF on the switch:

- `config ip ospf` commands (this page)
- `config ip ospf host-route` commands (page 3-12)
- `config ip ospf interface` commands (page 3-13)
- `config ip ospf area` commands (page 3-15)
- `config ip ospf area range` commands (page 3-16)

- `config ip ospf area virtual-interface` commands (page 3-17)

config ip ospf Commands

Use the `config ip ospf` commands to configure global OSPF parameters for the Passport 8000 Series switch as follows:

config ip ospf followed by:	
`info`	Displays the current OSPF configuration on the switch.
`admin-state <enable|disable>`	Globally enables or disables the OSPF administrative status. The default is disable.
`as-boundary-router <enable|disable>`	Enables or disables the OSPF Autonomous System boundary router.
`auto-vlink <enable|disable>`	Enables or disables automatic creation of OSPF virtual links when required. The default is disable.
`default-metric [ethernet <value>] [fast-ethernet <value>] [gig-ethernet <value>]`	Sets the OSPF default metrics. The range is 1 to 65535. • `[ethernet <value>]` is for the 10 Mb/s Ethernet (default is 100). • `[fast-ethernet <value>]` is the 100 Mb/s (fast) Ethernet (default is 10). • `[gig-ethernet <value>]` is the Gigabit (gig) Ethernet (default is 1).
`disable`	Globally disables OSPF on the switch.
`enable`	Globally enables OSPF on the switch.
`holddown <seconds>`	Sets the OSPF holddown timer value in seconds. • `<seconds>` is the range of seconds from 3 to 60; default is 10.
`router-id <ipaddr>`	Sets the OSPF router ID IP address. • `<ipaddr>` is the IP address.
`trap <enable|disable>`	Enables or disables issuing traps relating to OSPF.

Figure 3-8 shows a sample of the `config ip ospf info` command.

```
Passport-8610/config# ip ospf info

Sub-Context: bootconfig cli diag ethernet ip ipx log mlt rmon stg sys vlan
web-server qos
Current Context:

                admin-state : disable
          as-boundary-router : disable
              default-metric :
                          ethernet - 100
                     fast-ethernet - 10
                      gig-ethernet - 1
                  auto-vlink : disable
                    holddown : 10
                        trap : disable
                   router_id : 45.57.240.0
                      enable : false
```

Figure 3-8. *config ip ospf info* Command Output

config ip ospf host-route Commands

Use the `config ip ospf host-route` commands to configure OSPF host route parameters for the Passport 8000 Series switch.

The syntax includes the IP address `<ipaddr>` of the host router and the following parameters:

config ip ospf host-route <ipaddr> followed by:	
`info`	Displays the current OSFP host-route configuration on the switch.
`create`	Creates an OSPF host route for the IP address.
`delete`	Deletes an OSPF host route for the IP address.
`metric <metric>`	Sets the metric (cost) for the host route. • `<metric>` is between 1 and 65535.

config ip ospf interface Commands

These commands configure an OSPF interface where the interface <ipaddr> is represented by an IP address {a.b.c.d}.

The commands use the following syntax and parameters:

config ip ospf interface <ipaddr> followed by:	
info	Displays OSPF characteristics for the interface.
add-message-digest-key <md5-key-id> md5-key <value>	Adds an md5 key to the interface. At most, two md5 keys can be configured to an interface. Multiple md5 key configurations are used for md5 transitions without bringing down an interface.
admin-status <enable|disable>	Sets the state (enabled or disabled) of the OSPF interface.
area <ipaddr>	Sets the OSPF interface area. • <ipaddr> is a dotted-decimal notation to specify the area name. **Note:** The area name is not related to an IP address. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
authentication-key <authentication-key>	Sets the authentication key for the OSPF interface. • <authentication-key> is a string that specifies the key in up to eight characters.
authentication-type <auth-type>	Sets the OSPF authentication type for the interface. • <auth-type> is none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the *interface authentication-key* command. If MD5, they must contain the md5 key.
dead-interval <seconds>	Sets the OSPF dead interval for the interface. • <seconds> is the number of seconds the switch's OSPF neighbors should wait before assuming that this OSPF router is down. The range is from 1 to 2147483647. This value must be at least four times the hello interval value. The default is 40.
delete-message-digest-key <md5-key-id>	Deletes the specified md5 key ID from the configured md5 keys.

config ip ospf interface <ipaddr> followed by:	
hello-interval <seconds>	Sets the OSPF hello interval for the interface. • <seconds> is the number of seconds between hello packets sent on this interface. The range is 1 to 65535. The default is 10. **Note:** When you change the Hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency.
metric <metric>	Sets the OSPF metric for the interface. The switch advertises the metric in router link advertisements. • <metric> is the range 0 to 65535.
poll-interval <seconds>	Sets the polling interval for the OSPF interface in seconds. • <seconds> is between 1 and 2147483647.
priority <priority>	Sets the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1.
retransmit-interval <seconds>	Sets the retransmit interval for the OSPF interface, the number of seconds between link-state advertisement retransmissions. • <seconds> is between 1 and 3600.
transit-delay <seconds>	Sets the transit delay time for the OSPF interface, the estimated time in seconds it takes to transmit a link-state update packet over the interface. • <seconds> is between 1 and 3600.

Figure 3-9 shows a sample of the `config ip ospf interface info` command.

```
Passport-8610/config/ip/ospf/interface/130.1.1.1# info

Sub-Context:
Current Context:

   add-message-digest-key :
             admin-status : enabled
                     area : 1.1.1.1
      authentication-key : password
     authentication-type : simple
delete-message-digest-key : N/A
           hello-interval : 10
            dead-interval : 40
                   metric : 200
            poll-interval : 120
                 priority : 1
     retransmit-interval : 5
            transit-delay : 1
```

Figure 3-9. *config ip ospf interface info* Command Output

config ip ospf area Commands

The `config ip ospf area` commands allow you to control the OSPF area parameters, where `<ipaddr>` is the address of an OSPF area. Use dotted-decimal notation to specify the area name. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

The commands use the following syntax and parameters:

config ip ospf area <ipaddr> followed by:	
`info`	Displays OSPF area characteristics.
`create`	Creates an OSPF area.
`delete`	Deletes an OSPF area.
`import-summaries <true|false>`	Sets the area's support for importing summary advertisements into a stub area. This field should be used only if the area stub is set to true.
`nssa <true|false>`	Sets a not so stubby area (true or false). An NSSA prevents flooding of normal route advertisements into the area by replacing them with a default route.

config ip ospf area <ipaddr> followed by:	
stub <true|false>	Sets the import external option for this area to be stub or not {true|false}. A stub area has only one exit point (router interface) out of the area.
stub-metric <stub-metric>	Stub default metric for this stub area, which is the cost from 0 to 16777215. This is the metric value applied at the indicated type of service.

Figure 3-10 shows the `config ip ospf area info` command.

```
Passport-8610# config ip ospf area 1.0.0.0 info

Sub-Context:
Current Context:

                     create :
                     delete : N/A
            import-summaries : true
                        nssa : false
                        stub : false
                 stub-metric : 1
```

Figure 3-10. *config ip ospf area info* Command Output

config ip ospf area range Commands

The `config ip ospf area range` commands allow you to control the OSPF area range parameters, where `<ipaddr>` is the identification of an OSPF area and `<ipaddr/mask>` is the IP address and subnet mask of the range.

The commands use the following syntax and parameters:

config ip ospf area <ipaddr> range <ipaddr/mask> followed by:	
create advertise-mode <value> lsa-type <value>	Creates an OSPF area range with the specified IP address and advertising mode.
delete	Deletes an OSPF area range.
info	Displays information about the OSPF area range settings.

config ip ospf area virtual-interface Commands

The `config ip ospf area virtual-interface` commands allow you to configure an OSPF area virtual interface. All of the commands have the following two required parameters:

- `<ipaddr>` is the identification of an OSPF area in dotted-decimal notation. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
- `virtual-interface <nbr>` is the OSPF router ID of the neighbor.

The commands use the following syntax and parameters:

`config ip ospf area <ipaddr> virtual-interface <nbr>` `followed by:`	
`info`	Displays current OSPF area virtual interface information.
`add-message-digest-key <md5-key-id> md5-key <value>`	Adds an md5 key to the interface. At most, two md5 keys can be configured to an interface. Multiple md5 key configurations are used for md5 transitions without bringing down an interface.
`authentication-key <authentication-key>`	Sets the authentication key. • `<authentication-key>` is a string that specifies the key in up to eight characters.
`authentication-type <auth-type>`	Sets the OSPF authentication type for the OSPF area. • `<auth-type>` is none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the *area authentication-key* command. If MD5, they must contain the md5 key.
`create`	Creates a virtual interface area identifier.
`dead-interval <seconds>`	Sets the dead interval for the virtual interface, the number of seconds that a router's hello packets have not been seen before its neighbors declare the router down. • `<seconds>` is between 1 and 214783647. This value must be at least four times the hello interval value. The default is 60.
`delete`	Deletes the virtual interface.

config ip ospf area <ipaddr> virtual-interface <nbr> followed by:	
delete-message-digest-key <md5-key-id>	Deletes the specified md5 key ID from the configured md5 keys.
hello-interval <seconds>	Sets the hello interval on the virtual interface for the length of time (in seconds) between the hello packets that the router sends on the interface. • <seconds> is between 1 and 65535. The default is 10.
retransmit-interval <seconds>	Sets the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions. • <seconds> is between 1 and 3600.
transit-delay <seconds>	Sets the transmit delay for the virtual interface, the estimated number of seconds it takes to transmit a link-state update over the interface. • <seconds> is between 1 and 3600.

Note: Both sides of the OSPF connection must use the same authentication type and key.

show ip ospf Commands

These commands display the switch OSPF parameters.

show ip ospf area Command

The `show ip ospf area` command displays the OSPF area parameters.

The command uses the syntax:

```
show ip ospf area
```

Figure 3-11 is a sample.

```
Passport-8610/show/ip/ospf# area

================================================================================
                                      Ospf Area
================================================================================
AREA_ID         STUB_AREA  NSSA          IMPORT_SUM ACTIVE_IFCNT
--------------------------------------------------------------------------------
0.0.0.0         false      false         true       0
1.1.1.1         false      false         true       1

STUB_COST SPF_RUNS  BDR_RTR_CNT ASBDR_RTR_CNT LSA_CNT   LSACK_SUM
--------------------------------------------------------------------------------
0         8         0           0             0         0
1         8         0           1             3         128484
```

Figure 3-11. *show ip ospf area* Command Output

show ip ospf ase Command

The `show ip ospf ase` command displays the OSPF Autonomous System External (ASE) link state advertisements.

The command uses the syntax:

```
show ip ospf ase [metric-type <value>]
```

Information is displayed for all metric types or for the type specified.

Figure 3-12 shows a sample of the output.

```
Passport-8610/show/ip/ospf# ase

================================================================================
                                    Ospf AsExternal Lsas
================================================================================

LSTYPE     LINKSTATEID     ADV_ROUTER      E_METRIC  ASE_FWD_ADDR    AGE  SEQ_NBR    CSUM
--------------------------------------------------------------------------------
AsExternal 199.100.1.0     45.57.236.0     0 10      0.0.0.0         608  0x80000001 0x4fb8
```

Figure 3-12. *show ip ospf ase* Command Output

show ip ospf default-metric Command

The `show ip ospf default-metric` command displays the OSPF default metric information for each type of port.

The command uses the syntax:

```
show ip ospf default-metric
```

Figure 3-13 is a sample.

```
Passport-8606# show ip ospf default-metric

================================================================================
                                        Ospf Default Metric
================================================================================
  10MbpsPortDefaultMetric: 100
 100MbpsPortDefaultMetric: 10
1000MbpsPortDefaultMetric: 1
```

Figure 3-13. *show ip ospf default-metric* Command Output

show ip ospf host-route Command

The `show ip ospf host-route` command displays the OSPF host route configuration including host IP address, type of service, and the metric used.

The command uses the syntax:

```
show ip ospf host-route
```

show ip ospf ifstats Command

The `show ip ospf ifstats` command displays IP OSPF interface statistics where the parameter `mismatch` is the number of times the area ID is not matched.

The command uses the syntax:

```
show ip ospf ifstats [mismatch] [detail]
```

The output format is shown in Figure 3-14.

```
Passport-8610/show/ip/ospf# ifstats

================================================================================
                                    Ospf Interface Statistics
================================================================================
               ---HELLOS---- ---DBS--- -LS REQ-- --LS UDP--- --LS ACK---
INTERFACE      RX     TX     RX   TX   RX   TX   RX    TX     RX    Tx
--------------------------------------------------------------------------------
130.1.1.1      86     85     8    3    1    1    13    1      2     1
```

Figure 3-14. *show ip ospf ifstats* Command Output

show ip ospf info Command

The `show ip ospf info` command displays the current OSPF settings for the switch.

The command uses the syntax:

```
show ip ospf info
```

Figure 3-15 is a sample display.

```
Passport-8610/show/ip/ospf# info

================================================================================
                                          Ospf General
================================================================================

          RouterId: 45.57.0.0
         AdminStat: enabled
     VersionNumber: 2
  AreaBdrRtrStatus: false
    ASBdrRtrStatus: false
    ExternLsaCount: 1
 ExternLsaCksumSum: 20408(0x4fb8)
        TOSSupport: 0
  OriginateNewLsas: 3
         RxNewLsas: 12
        TrapEnable: false
AutoVirtLinkEnable: false
   SpfHoldDownTime: 10
```

Figure 3-15. *show ip ospf info* Command Output

show ip ospf interface Command

The `show ip ospf interface` command displays information about the OSPF interface.

The command uses the syntax:

```
show ip ospf interface
```

Figure 3-16 is the output.

```
Passport-8610/show/ip/ospf# interface

================================================================================
                                    Ospf Interface
================================================================================
INTERFACE       AREAID          ADMINST IFST METR PRIO DR/BDR          AUTHKEY  AUTHTYPE
--------------------------------------------------------------------------------
130.1.1.1       1.1.1.1         enable  BDR  10   1    130.1.1.2               none
                                                      130.1.1.1


================================================================================
                                    Ospf Virtual Interface
================================================================================
AREAID          NBRIPADDR       STATE    AUTHKEY  AUTHTYPE
--------------------------------------------------------------------------------
```

Figure 3-16. *show ip ospf interface* Command Output

show ip ospf int-timers Command

The `show ip ospf int-timers` command displays the parameters for the OSPF interface timers.

The command uses the syntax:

```
show ip ospf int-timers
```

Figure 3-17 is the output.

```
Passport-8610# show ip ospf int-timers

================================================================================
                                    Ospf Interface Timer
================================================================================
                                TRANSIT  RETRANS  HELLO    DEAD     POLL
INTERFACE       AREAID          DELAY    INTERVAL INTERVAL INTERVAL INTERVAL
--------------------------------------------------------------------------------
10.10.40.3      0.0.0.0         1        5        10       40       120
```

Figure 3-17. *show ip ospf int-timers* Command Output

show ip ospf lsdb Command

The `show ip ospf lsdb` command displays the OSPF link state database (lsdb) table.

The command has the following format:

```
show ip ospf lsdb [area <value>] [lsatype <value>] [lsid <value>]
[adv_rtr <value>] [detail]
```

You can optionally specify an area string, link state advertisement type (0 to 5), link state ID, or advertising router. Adding `detail` to the command provides more details.

Figure 3-18 is a sample display of the command without any variables.

```
Passport-8610/show/ip/ospf# lsdb

================================================================================
                                        Ospf Lsdb
================================================================================

               Router Lsas in Area 1.1.1.1

LSTYPE     LINKSTATEID     ADV_ROUTER      AGE  SEQ_NBR    CSUM
--------------------------------------------------------------------------------
Router     45.57.0.0       45.57.0.0       1028 0x80000003 0x8be3
Router     45.57.236.0     45.57.236.0     586  0x8000000a 0xa402

               Network Lsas in Area 1.1.1.1

LSTYPE     LINKSTATEID     ADV_ROUTER      AGE  SEQ_NBR    CSUM
--------------------------------------------------------------------------------
Network    130.1.1.2       45.57.236.0     1034 0x80000001 0xc5ff
```

Figure 3-18. *show ip ospf lsdb* Command Output

Figure 3-19 is a sample output of the `show ip ospf lsdb` command with the `detail` option.

```
Passport-8610/show/ip/ospf# lsdb detail

================================================================================
                                      Ospf Lsdb
================================================================================

Router Link LSA :
Area           : 1.1.1.1 (0x1010101)
Age            : 1123
Opt            : true (External Routing Capability)
Type           : 1
LsId           : 45.57.0.0 (0x2d390000)
Rtr            : 45.57.0.0
Seq            : -2147483645 (0x80000003)
Csum           : 35811 (0x8be3)
Len            : 36
ABR            : false
ASBR           : false
Vlnk           : false (endpoint of active Vlink)
#Lnks          : 1
[1]
Id             : 130.1.1.2 (0x82010102)
Data           : 130.1.1.1 (0x82010101)
Type           : (conn-to-transmit-net)(Id=DR-Addr, Data=Rtr-Addr)
Met            : 10

Router Link LSA :
Area           : 1.1.1.1 (0x1010101)
Age            : 697
Opt            : true (External Routing Capability)
Type           : 1
LsId           : 45.57.236.0 (0x2d39ec00)
Rtr            : 45.57.236.0
Seq            : -2147483638 (0x8000000a)
Csum           : 41986 (0xa402)
Len            : 48
ABR            : false
ASBR           : true
Vlnk           : false (endpoint of active Vlink)
#Lnks          : 2
[1]
Id             : 200.1.1.0 (0xc8010100)
Data           : 255.255.255.0 (0xffffff00)
Type           : (conn-to-stub-net)(Id=Subnet-Prefix, Data=Prefix-Len)
#Tos           : 0
Met            : 10
Id             : 130.1.1.2 (0x82010102)
Data           : 130.1.1.2 (0x82010102)
Type           : (conn-to-transmit-net)(Id=DR-Addr, Data=Rtr-Addr)
#Tos           : 0
Met            : 10
```

```
Network Link LSA :
Area           : 1.1.1.1 (0x1010101)
Age            : 1156
Opt            : true (External Routing Capability)
Type           : 2
LsId           : 130.1.1.2 (0x82010102)
Rtr            : 45.57.236.0
Seq            : -2147483647 (0x80000001)
Csum           : 50687 (0xc5ff)
Len            : 32
Mask           : 255.255.0.0
#Rtr           : 2
[1]            : 45.57.236.0
[2]            : 45.57.0.0
```

Figure 3-19. *show ip ospf lsdb detail* Command Output

show ip ospf neighbors Command

The `show ip ospf neighbors` command displays OSPF neighbors with the information shown in Figure 3-20.

The command uses the syntax:

`show ip ospf neighbors`

Figure 3-20 is an output.

```
Passport-8610/show/ip/ospf# neighbors

================================================================================
                                    Ospf Neighbors
================================================================================
INTERFACE       NBRROUTERID     NBRIPADDR       PRIO_STATE    RTXQLEN
--------------------------------------------------------------------------------
130.1.1.1       45.57.236.0     130.1.1.2       1    Full     0

================================================================================
                                    Ospf Virtual Neighbors
================================================================================
NBRAREAID       NBRROUTERID     NBRIPADDR       STATE    RTXQLEN
--------------------------------------------------------------------------------
1.1.1.1         45.57.236.0     130.1.1.2       Full     0
```

Figure 3-20. *show ospf neighbors* Command Output

show ip ospf range Command

The `show ip ospf range` command displays the OSPF range including area ID, range network address, range subnet mask, range flag, and LSDB type.

show ip ospf stats Command

The `show ip ospf stats` command displays the OSPF statistics.

The command uses the syntax:
`show ip ospf stats`

Figure 3-21 shows a sample output.

```
Passport-8610/show/ip/ospf# stats

=========================================================================
                                          Ospf Statistics
=========================================================================

    NumBufAlloc: 119
     NumBufFree: 119
NumBufAllocFail: 0
 NumBufFreeFail: 0
       NumTxPkt: 120
       NumRxPkt: 131
   NumTxDropPkt: 0
   NumRxDropPkt: 0
    NumRxBadPkt: 0
      NumSpfRun: 9
     LastSpfRun: 0x1e0dc
    LsdbTblSize: 4
```

Figure 3-21. *show ip ospf stats* Command Output

config ethernet <ports> ip ospf Commands

The port-based OSPF commands set OSPF parameters for a specific port. The parameter <ports> specifies the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.

The config ethernet <ports> ip ospf commands use the following syntax and parameters:

config ethernet <ports> ip ospf followed by:	
info	Displays OSPF characteristics on the port.
advertise-when-down <enable|disable>	If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. **Note**: When you configure a port without any link and enable advertise-when-down, the route is not advertised until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter should be disabled.
area <ipaddr>	Sets the OSPF identification number for the area, typically formatted as an IP address.
authentication-key <string>	Sets the authentication key for the port (OSPF interface). • <string> specifies the key as a simple password with eight characters.
authentication-type <auth-type>	Sets the OSPF authentication type for the port: none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the *area authentication-key* command. If MD5, they must contain the md5 key.
disable	Disables OSPF on the port.

config ethernet <ports> ip ospf followed by:	
dead-interval <seconds>	Sets the router OSPF dead interval—the number of seconds the switch's OSPF neighbors should wait before assuming that the OSPF router is down. • <seconds> is a value from 1 to 2147836437; the default is 40. The value must be at least four times the hello interval.
enable	Enables OSPF on the port.
hello-interval <seconds>	Sets the OSPF hello interval, which is the number of seconds between hello packets sent on this interface. • <seconds> is a value from 1 to 65535. The default is 10.
metric <cost>	Sets the OSPF metric associated with this interface and advertised in router link advertisements. • <cost> is in the range from 0 to 65535; the default is 0.
priority <integer>	Sets the OSPF priority for the port during the election process for the designated router. The port with the highest priority number is the best candidate for the designated router. If you set the priority to 0, the port cannot become either the designated router or a backup designated router. • <integer> is between 0 and 255. The default is 1.

Note: Both sides of the OSPF connection must use the same authentication type and key.

Figure 3-22 shows a sample of the `config ethernet ip ospf info` command.

```
Passport-8610# config ethernet 9/2 ip ospf info

Sub-Context:
Current Context:

Port 9/2 :
         advertise-when-down : disable
                        ospf : enable
              hello-interval : 10
               dead-interval : 40
                    priority : 1
                      metric : 0
         authentication-type : none
          authentication-key :
                        area : 1.0.0.0
```

Figure 3-22. *config ethernet ip ospf info* Command Output

show ports ospf Commands

These commands display OSPF parameters and statistics for a port or all ports.

show ports error ospf Command

The `show ports error ospf` command displays extended information about OSPF errors for the specified port or for all ports.

The command uses the syntax:

```
show ports error ospf [<ports>]
```

Figure 3-23 is a sample display.

```
Passport-8610# show ports error ospf

================================================================================
                                    Port Ospf Error
================================================================================
PORT  VERSION  AREA     AUTHTYPE AUTH     NET_MASK HELLOINT DEADINT  OPTION
NUM   MISMATCH MISMATCH MISMATCH FAILURES MISMATCH MISMATCH MISMATCH MISMATCH
--------------------------------------------------------------------------------
9/1   0        0        0        0        0        0        0        0
9/13  0        0        0        0        0        0        0        0
```

Figure 3-23. *show ports error ospf* Command Output

show ports info ospf Command

The `show ports info ospf` command displays information about the OSPF parameters of the specified port or all ports.

The command uses the format:

```
show ports info ospf [<ports>]
```

Figure 3-24 is an example.

```
Passport-8610# show ports info ospf

================================================================================
                                        Port Ospf
================================================================================
PORT          HELLO   RTRDEAD OSPF
NUM   ENABLE  INTVAL  INTVAL  PRIORITY METRIC AUTHTYPE AUTHKEY    AREA_ID
--------------------------------------------------------------------------------
9/1   false   10      40      1        0      none                0.0.0.0
9/2   true    10      40      1        0      none                1.0.0.0
9/3   false   10      40      1        0      none                0.0.0.0
9/4   false   10      40      1        0      none                0.0.0.0
9/5   false   10      40      1        0      none                0.0.0.0
9/6   false   10      40      1        0      none                0.0.0.0
9/7   false   10      40      1        0      none                0.0.0.0
9/8   false   10      40      1        0      none                0.0.0.0
9/9   false   10      40      1        0      none                0.0.0.0
```

Figure 3-24. *show ports info ospf* Command (Partial Output)

show ports stats ospf main Command

The `show ports stats ospf main` command displays basic OSPF information about the specified port or for all ports.

The command uses the syntax:

```
show ports stats ospf main [<ports>]
```

Figure 3-25 is a sample display.

```
Passport-8610# show ports stats ospf main

================================================================================
                                    Port Stats Ospf
================================================================================
PORT_NUM RX_HELLO   TX_HELLO   RXDB_DESCR TXDB_DESCR RXLS_UPDATE   TXLS_UPDATE
--------------------------------------------------------------------------------
9/2      0          0          0          0          0             0
9/3      0          0          0          0          0             0
```

Figure 3-25. *show ports stats ospf main* Command Output

show ports stats ospf extended Command

The `show ports stats ospf extended` command displays extended OSPF information about the specified port or for all ports.

The command uses the syntax:

`show ports stats interface extended [<ports>]`

config vlan <vid> ip ospf Commands

The `config vlan <vid> ip ospf` commands set OSPF parameters for the specified VLAN (`<vid>` is 1 to 4094).

The commands use the following syntax and parameters:

config vlan <vid> ip ospf followed by:	
`info`	Displays OSPF characteristics on the VLAN.
`advertise-when-down <enable|disable>`	If enabled, the network on this interface is advertised as up, even if no ports in the VLAN are active. The default is disabled. **Note**: When you create a VLAN with no active ports and enable advertise-when- down, the route is not advertised until a port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, disable this parameter.
`area <ipaddr>`	Sets the OSPF interface area ID for the VLAN.

config vlan <vid> ip ospf followed by:	
authentication-key <string>	Sets the authorization key for the VLAN. • <string> is key of a string with up to eight characters.
authentication-type <auth-type>	Sets the OSPF authentication type for the VLAN. • <auth-type> is none, simple password, or MD5 authentication. If simple, all OSPF updates received by the VLAN must contain the authentication key specified by the *area authentication-key* command. If MD5, they must contain the md5 key.
disable	Disables OSPF on the VLAN.
dead-interval <seconds>	Sets the OSPF dead interval for the VLAN, the number of seconds the switch's OSPF neighbors should wait before assuming that this OSPF router is down. • <seconds> is the range from 1 to 2147483647. This value must be at least four times the hello interval value. The default is 40.
enable	Enables OSPF on the VLAN.
hello-interval <seconds>	Sets the OSPF hello interval for the VLAN, the number of seconds between hello packets sent on this VLAN. • <seconds> is the range 1 to 65535. The default is 10.
metric <cost>	Sets the OSPF metric for the VLAN. The switch advertises the metric in router link advertisements. • <seconds> is the range 0 to 65535. The default is 0.
priority <integer>	Sets the OSPF priority for the VLAN during the election process for the designated router. The VLAN with the highest priority number is the best candidate for the designated router. If the priority is 0, the VLAN cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. • <integer> is the range 0 to 255. The default is 1.

Note: Both sides of the OSPF connection must use the same authentication type and key.

Figure 3-26 shows the output of the `config vlan ip ospf info` command.

```
Passport-8610# config vlan 2 ip ospf info

Sub-Context: clear config dump monitor show test trace
Current Context:

         advertise-when-down : disable
                        ospf : enable
              hello-interval : 10
               dead-interval : 40
                    priority : 1
                      metric : 10
         authentication-type : none
          authentication-key :
                        area : 0.0.0.0
```

Figure 3-26. *config vlan ip ospf info* Command Output

show vlan info ospf Command

The `show vlan info ospf` command shows the OSPF parameters configured for all VLANs or the specified VLAN.

The command uses the syntax:

```
show vlan info ospf [<vid>]
```

Figure 3-27 is a sample.

```
Passport-8610# show vlan info ospf

================================================================================
                                    Vlan Ospf
================================================================================
VLAN        HELLO    RTRDEAD  DESIGRTR
ID  ENABLE INTERVAL INTERVAL PRIORITY METRIC AUTHTYPE AUTHKEY    AREAID
--------------------------------------------------------------------------------
1   false  10       40       1        0      none               0.0.0.0
2   true   10       40       1        10     none               0.0.0.0
3   false  10       40       1        0      none               0.0.0.0
4   false  10       40       1        0      none               0.0.0.0
```

Figure 3-27. *show vlan info ospf* Command Output

Chapter 4
VRRP Commands

This chapter describes the Run-Time CLI commands that are used to configure VRRP layer 3 (routing) functions in the Passport 8000 Series switch.

VRRP Commands

Virtual Router Redundancy Protocol (VRRP) is designed to eliminate an inherent failure in the static default routed environment by introducing a logical IP address shared between two or more routers connecting the subnet to the enterprise network.

config ethernet <ports> ip vrrp Commands

The `config ethernet <ports> ip vrrp <vrid>` commands allow you to set VRRP on a port. These commands use the following parameters:

- `<ports>` specify the ports for which you are entering the command in the form portlist {slot/port[-slot/port][, ...]}.
- `<vrid>` is the virtual router ID (1 to 255), a number that uniquely identifies a virtual router on a given VRRP router. The virtual router acts as the default router for one or more assigned addresses.

The commands use the following syntax and parameters:

config ethernet <ports> ip vrrp <vrid> followed by:	
info	Displays the current port VRRP configuration.
address <ipaddr>	Sets the IP address of the virtual router interface.
adver-int <seconds>	Sets the advertising interval (in seconds), the time interval between sending VRRP advertisement messages. The value must be the same on all participating routers. The range is 1 to 255, and the default is 1.
critical-ip <ipaddr>	Sets the critical IP address for VRRP. This address is an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface went down).
delete	Deletes VRRP from the port.
disable	Disables VRRP on the port.
enable	Enables VRRP on the port.
priority <prio>	Sets the port VRRP priority (1 to 254) value to be used by this VRRP router. The default is 100. The value 255 is assigned to the router that owns the IP address associated with the virtual router.

Figure 4-1 shows the `config ethernet ip vrrp info` command.

```
Passport-8610# config ethernet 3/2 ip vrrp 1 info

Sub-Context:
Current Context:

Port 3/2 :
                    address : 10.10.40.10
                  adver-int : 1
                critical-ip : 10.10.40.15
                     delete : N/A
                       vrrp : enable
                   priority : 100
```

Figure 4-1. *config ethernet ports ip vrrp info* Command Output

show port vrrp Commands

The following commands display port VRRP configuration and statistics.

show ports info vrrp main Command

The `show ports info vrrp main` command displays basic VRRP configuration information about the specified port or for all ports.

The command uses the syntax:

```
show ports info vrrp main [<ports>]
```

show ports info vrrp extended Command

The `show ports info vrrp extended` command displays extended VRRP configuration information about the specified port or for all ports.

The command uses the syntax:

```
show ports info vrrp extended [<ports>]
```

Figure 4-2 is a sample output, and in it, the Master_IPaddr is the IP address of the master router.

```
Passport-8610# show ports info vrrp extended

================================================================================
                                    Port Vrrp Extended
================================================================================
PORT  STATE      CONTROL  PRIORITY  MASTER_IPADDR   ADVERTISE CRITICAL_IPADDR
--------------------------------------------------------------------------------
3/3   master     enabled  255       200.200.200.1   1         0.0.0.0
```

Figure 4-2. *show ports info vrrp extended* Command Output

show ports stats vrrp Command

The `show ports stats vrrp` command displays VRRP information about the specified port or for all ports.

The command uses the syntax:

```
show ports stats vrrp [<ports>]
```

config vlan <vid> ip vrrp Commands

The `config vlan <vid> ip vrrp <vrid>` commands allow you to set VRRP on a VLAN using these required parameters:

- `<vid>` is the VLAN ID (1 to 4094).
- `<vrid>` is the virtual router ID (1 to 255), a number that uniquely identifies a virtual router on a given VRRP router. The virtual router acts as the default router for one or more assigned addresses.

The VLAN VRRP commands use the following syntax and parameters:

config vlan <vid> ip vrrp <vrid> followed by:	
`info`	Displays the current VLAN VRRP settings.
`address <ipaddr>`	Sets the IP address of the virtual router interface.
`adver-int <seconds>`	Sets the advertising interval (in seconds), the time interval between sending advertisement messages. • `<seconds>` is the range 1 to 255, and the default is 1.
`critical-ip <ipaddr>`	Sets the critical IP address for VRRP. This address is an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface went down).
`delete`	Deletes the VRRP from the VLAN.
`disable`	Disables the VRRP on the VLAN.
`enable`	Enables VRRP on the VLAN.
`priority <prio>`	Sets the port VRRP priority value to be used by this VRRP router. • `<prio>` is between 1 and 254. The default is 100. The value 255 is assigned to the router that owns the IP address associated with the virtual router.

Figure 4-3 shows a sample of the `config vlan ip vrrp info` command.

```
Passport-8610# config vlan 2 ip vrrp 1 info

Sub-Context:
Current Context:

                    address : 100.100.100.1
                  adver-int : 1
                critical-ip : 0.0.0.0
                     delete : N/A
                vrrp enable : disable
                   priority : 100
```

Figure 4-3. *config vlan ip vrrp info* Command Output

show vlan vrrp Commands

Two show commands display VLAN VRRP information.

show vlan info vrrp main Command

The `show vlan info vrrp main` command displays the basic VRRP configuration for all VLANs on the switch or for the specified VLAN.

The command uses the syntax:

`show vlan info vrrp main [<vid>]`

Figure 4-4 is a sample output.

```
Passport-8610# show vlan info vrrp main

================================================================================
                                    Vlan Vrrp
================================================================================
VLAN VRRP                VIRTUAL
ID   ID   IPADDR         MAC ADDR
--------------------------------------------------------------------------------
2    1    100.100.100.1  00:00:5e:00:01:01
```

Figure 4-4. *show vlan info vrrp main* Command Output

show vlan info vrrp extended Command

The `show vlan info vrrp extended` command displays the extended VRRP configuration for all VLANs on the switch or for the specified VLAN.

The command uses the syntax:

```
show vlan info vrrp extended [<vid>]
```

Figure 4-5 is a sample output.

```
Passport-8610# show vlan info vrrp extended

================================================================================
                                    Vlan Vrrp Extended
================================================================================
                                 MASTER          ADVERTISE CRITICAL
VID  STATE      CONTROL  PRIORITY  IPADDR          INTERVAL  IPADDR
--------------------------------------------------------------------------------
2    initialize disabled 100       0.0.0.0         1         0.0.0.0
```

Figure 4-5. *show vlan info vrrp extended* Command Output

show ip vrrp Commands

These commands display information about VRRP as configured on the switch.

show ip vrrp info Command

The `show ip vrrp info` command displays VRRP information on the interface. If a virtual router ID or an IP address is entered, the information will be displayed only for that VRID or that interface; if not, all VRRP interfaces are listed.

This command uses the syntax:

```
show ip vrrp info [<vrid>] [<ipaddr>]
```

Figure 4-6 is a sample output.

```
Passport-8610# show ip vrrp info

================================================================================
                                    Vrrp Info
================================================================================

VRID  IP              MAC               STATE    CONTROL  PRIO
--------------------------------------------------------------------------------
1     100.100.100.1   00:00:5e:00:01:01  Init     Disabled 100

VRID  MASTER          ADV    UP                   CRITICAL
--------------------------------------------------------------------------------
1     0.0.0.0         1      0 day(s), 00:00:00   0.0.0.0
```

Figure 4-6. *show ip vrrp info* Command Output

show ip vrrp stats Command

The `show ip vrrp stats` command displays counter information for the specified VRRP or all VRRP interfaces. You must enter a VRID (virtual router ID) and an IP address.

This command uses the format:

```
show ip vrrp stats <vrid> <ipaddr>
```

Chapter 5
IP Multicast Commands

This chapter describes the Run-Time CLI commands that are used to configure multicasting functions in the Passport 8000 Series switch. The chapter includes sections about the following command groups used to configure routing characteristics:

- IP Multicast Commands
- DVMRP Commands
- Layer 3 IGMP Commands

IP Multicast Commands

The IP multicast commands allow you to configure and view IP multicasting parameters on the switch.

config ip mroute Commands

The commands to configure multicast routing on the switch take the following syntax and format, where `<ipaddr>` is the multicast route interface IP address:

config ip mroute followed by:	
`info`	Displays information about the multicast route.
`interface <ipaddr> info`	Displays information about the multicast route interface.
`mroute interface <ipaddr> ttl <ttl>`	Sets the default time-to-live threshold for the multicast route interface.

show ip mroute Commands

These commands display information about the multicast route(s) set up on the switch.

show ip mroute interface Command

The `show ip mroute interface` command displays information about the multicast interface.

The command uses the syntax:

```
show ip mroute interface
```

Figure 5-1 is a sample display.

```
Passport-8610# show ip mroute interface

=================================================================
                                          Mroute Interface
=================================================================
INTERFACE  TTL   PROTOCOL
-----------------------------------------------------------------
Vlan20     1     dvmrp
Vlan21     1     dvmrp
```

Figure 5-1. *show ip mroute interface* Command Output

show ip mroute next-hop Command

The `show ip mroute next-hop` command displays information about the next hop for the multicast route.

The command uses the syntax:

```
show ip mroute next-hop
```

Figure 5-2 is a sample display.

```
Passport-8610# show ip mroute next-hop

=============================================================================
                                    Mroute Next Hop
=============================================================================
INTERFACE  GROUP           SOURCE          SRCMASK         ADDRESS
-----------------------------------------------------------------------------
INTERFACE  STATE      EXPIRY_TIME     CLOSE_HOP       PRIORITY
-----------------------------------------------------------------------------
```

Figure 5-2. *show ip mroute next-hop* Command Output

show ip mroute route Command

The `show ip mroute route` command displays information about the multicast route.

The command uses the syntax:

```
show ip mroute route
```

Figure 5-3 displays the headings found in the multicast route table.

```
Passport-8610# show ip mroute route
================================================================================
                                    Mroute Route
================================================================================
GROUP           SOURCE          SRCMASK         UPSTREAM_NBR    IF    EXPIR PROT
--------------------------------------------------------------------------------
```

Figure 5-3. *show ip mroute route* Command Output

show ports stats routing Command

The `show ports stats routing` command displays routing (unicast and multicast) information about the specified port or for all ports.

The command uses the syntax:

```
show ports stats routing [<ports>]
```

Figure 5-4 is a sample display.

```
Passport-8610# show ports stats routing

================================================================================
                                    Port Stats Routing
================================================================================
PORT     IN_FRAME    IN_FRAME    IN          OUT_FRAME   OUT_FRAME
NUM      UNICAST     MULTICAST   DISCARD     UNICAST     MULTICAST
--------------------------------------------------------------------------------
1/1      4294832127 4294967039 4294827993 0          0
1/2      4294963199 4294705151 3952869371 0          0
1/3      4292870143 3758096383 3758088157 0          0
1/4      4273930239 4277926911 3221220665 0          0
1/5      4294967295 4294967039 2071903849 0          0
1/6      4294967295 4294966783 4160192501 0          0
1/7      4294967295 4294967295 4227792893 0          0
1/8      4294965247 3724541951 4294957053 0          0
1/9      4160749567 4294966655 4160217083 0          0
1/10     0          0          0          0          0
1/11     4261412863 4294443007 4294966781 0          0
```

Figure 5-4. *show ports stats routing* Command (Partial Output)

DVMRP Commands

Distance Vector Multicast Routing Protocol (DVMRP) is used between routers to exchange their multicast routing information. The protocol can be configured on a VLAN, but it must be enabled globally in order to take effect.

config ip dvmrp Commands

These commands are the global DVMRP commands.

config ip dvmrp Commands

The `config ip dvmrp` commands use the following syntax and parameters:

`config ip dvmrp` `followed by:`	
`info`	Displays DVMRP settings on the switch.
`disable`	Globally disables DVMRP on the switch.
`enable`	Globally enables DVMRP on the switch.

config ip dvmrp followed by:	
leaf-timeout <integer>	Sets the length of time (in seconds) the router waits for a response from a neighbor before considering the attached network to be a leaf network. • <integer> is the range of 25 to 4000; the default is 200.
nbr-timeout <integer>	Sets the length of time (in seconds) the router waits to receive a report from a neighbor before considering the connection inactive. • <integer> is the range of 35 to 8000; the default is 35.
nbr-probe-interval <integer>	Sets the time interval (in seconds) for the DVMRP router to send a neighbor probe message on its interface. • <integer> is the range of 5 to 30 seconds; the default is 10.
triggered-update-interval <integer>	Sets the time interval (in seconds) between triggered update messages sent when routing information changes. • <integer> is the range of 5 to 1000; the default is 5.
update-interval <integer>	Sets the time interval (in seconds) between DVMRP router update messages. • <integer> is the range of 10 to 2000; the default is 60.

Figure 5-5 shows a sample of the `config ip dvmrp info` command.

```
Passport-8610# config ip dvmrp info

Sub-Context:
Current Context:

                      enable : true
             update-interval : 60
   triggered-update-interval : 5
                leaf-timeout : 200
                 nbr-timeout : 35
          nbr-probe-interval : 10
```

Figure 5-5. *config ip dvmrp info* Command Output

config ip dvmrp interface Commands

The `config ip dvmrp interface` commands require an IP address `<ipaddr>` and use the following syntax and parameters:

`config ip dvmrp interface <ipaddr>` `followed by:`	
`info`	Displays information about the specified DVMRP local router interface.
`disable`	Disables DVMRP on the local router interface.
`enable`	Enables DVMRP on the local router interface.
`metric <cost>`	Sets the cost metric (maximum number of hops) for the router interface. • `<cost>` is the range of 1 to 31.

show ip dvmrp Commands

These commands display information about DVMRP as set on the switch.

show ip dvmrp info Command

The `show ip dvmrp info` command displays information about the general DVMRP group.

The command uses the syntax:

```
show ip dvmrp info
```

Figure 5-6 is a sample display.

```
Passport-8610# show ip dvmrp info

================================================================================
                                        Dvmrp General Group
================================================================================
AdminStat               : enabled
Genid                   : 152
Version                 : 3
NumRoutes               : 0
NumReachableRoutes      : 0

UpdateInterval          : 60
TriggeredUpdateInterval : 5
LeafTimeOut             : 200
NbrTimeOut              : 35
NbrProbeInterval        : 10
```

Figure 5-6. *show ip dvmrp info* Command Output

show ip dvmrp interface Command

The `show ip dvmrp interface` command displays information about the DVMRP interface set up on the switch.

The command's syntax is:

```
show ip dvmrp interface
```

Figure 5-7 is a sample output.

```
Passport-8610/show/ip/dvmrp# interface

================================================================================
                                    Dvmrp Interface
================================================================================
IF        ADDR            METRIC     OPERSTAT
--------------------------------------------------------------------------------
Port7/1   10.160.192.45   1 down
Vlan2     10.108.96.45    1          down
Vlan3     10.108.97.45    1          down
Vlan4     10.108.98.45    1          down
Vlan5     10.108.99.45    1          down
Vlan6     10.108.100.45   1          down
Vlan10    10.108.104.45   1          down
Vlan15    10.108.109.45   1          down
Vlan18    10.108.112.45   1          down
Vlan23    10.108.126.27   1          down
Vlan27    10.108.115.1    1          down
Vlan51    10.108.117.1    1          down
Vlan52    10.28.1.20      1          up
```

Figure 5-7. *show ip dvmrp interface* Command Output

show ip dvmrp neighbor Command

The `show ip dvmrp neighbor` command displays information about the configured DVMRP neighbor, including the interface, address, expiration time, GENID, major and minor version number, capability, and state.

The command's syntax is:

```
show ip dvmrp neighbor
```

show ip dvmrp next-hop Command

The `show ip dvmrp next-hop` command displays information about the DVMRP next hops.

The command's syntax is:

```
show ip dvmrp next-hop
```

Figure 5-8 is a sample output.

```
Passport-8610/show/ip/dvmrp# next-hop

================================================================================
                                    Dvmrp Next Hop
================================================================================
SOURCE          MASK            INTERFACE  TYPE
--------------------------------------------------------------------------------
10.160.140.0   255.255.255.0   Vlan52     leaf
10.28.1.0      255.255.255.0   Vlan52
```

Figure 5-8. *show ip dvmrp next-hop* Command Output

show ip dvmrp route Command

The `show ip dvmrp route` command displays information about the DVMRP routes.

The command's syntax is:

```
show ip dvmrp route
```

Figure 5-9 is a sample output.

```
Passport-8610/show/ip/dvmrp# route

================================================================================
                                    Dvmrp Route
================================================================================
SOURCE          MASK            UPSTREAM_NBR    INTERFACE  METRIC EXPIRE
--------------------------------------------------------------------------------
10.160.140.0   255.255.255.0   0.0.0.0         Vlan53     32     115
10.28.1.0      255.255.255.0   0.0.0.0         Vlan52     1      215
```

Figure 5-9. *show ip dvmrp route* Command Output

config ethernet <ports> ip dvmrp Commands

The `config ethernet <ports> ip dvmrp` commands allow you to configure DVMRP at the port level. DVMRP must be enabled globally for these settings to take effect.

The DVMRP port commands require the parameter <ports> as the port or list of ports for the command {slot/port[-slot/port][, ...]} and use the following syntax and commands:

config ethernet <ports> ip dvmrp followed by:	
info	Displays DVMRP settings on the port.
enable	Enables DVMRP on the port.
disable	Disables DVMRP on the port.
metric <cost>	Sets the DVMRP route metric. • <cost> is the maximum number of hops with a value of 1 to 31.

Figure 5-10 shows a sample of the config ethernet <ports> ip dvmrp info command.

```
Passport-8610# config ethernet 9/3 ip dvmrp info

Sub-Context:
Current Context:

                      dvmrp : disable
                     metric : 1
```

Figure 5-10. *config ethernet ip dvmrp info* Command Output

show ports info dvmrp Command

The show ports info dvmrp command displays information about DVMRP configuration for the specified port or for all ports.

This command uses the format:

```
show ports info dvmrp [<ports>]
```

Figure 5-11 is a sample.

```
Passport-8610# show ports info dvmrp

================================================================================
                                        Port Ip Dvmrp
================================================================================
PORT-NUM        DVMRP-ENABLE    METRIC
--------------------------------------------------------------------------------
9/1             disable         1
9/2             disable         1
9/3             disable         1
9/4             disable         1
9/5             disable         1
9/6             disable         1
9/7             disable         1
9/8             disable         1
```

Figure 5-11. *show ports info dvmrp* Command Output

config vlan <vid> ip dvmrp Commands

The `config vlan ip dvmrp` commands configure DVMRP on the VLAN (`<vid>` from 1 to 4094) and use the following syntax and parameters:

config vlan <vid> ip dvmrp followed by:	
`info`	Displays DVMRP settings on the VLAN.
`enable`	Enables DVMRP on the VLAN.
`disable`	Disables DVMRP on the VLAN.
`metric <cost>`	Sets the DVMRP route metric. • `<cost>` is the maximum number of hops with a value of 1 to 31.

Figure 5-12 shows a sample of the `config vlan ip dvmrp info` command.

```
Passport-8610# config vlan 1 ip dvmrp info

Sub-Context:
Current Context:

                      dvmrp : enable
                     metric : 1
```

Figure 5-12. *config vlan ip dvmrp info* Command Output

show vlan info dvmrp Command

The `show vlan info dvmrp` command displays the DVMRP configuration for all VLANs or the specified VLAN.

The command uses the syntax:

```
show vlan info dvmrp [<vid>]
```

A sample output is shown in Figure 5-13.

```
Passport-8610# show vlan info dvmrp

================================================================================
                                        Vlan Ip Dvmrp
================================================================================
VLAN-ID         DVMRP-ENABLE    METRIC
--------------------------------------------------------------------------------
1               enable          1
```

Figure 5-13. *show vlan info dvmrp* Command Output

Layer 3 IGMP Commands

The Internet Group Management Protocol (IGMP) is used by hosts to report their multicast group memberships to neighbor multicast routers. DVMRP multicasting must be enabled globally on the switch for these commands to take effect. IGMP configuration is on a per interface basis.

config ip l3-igmp Commands

These commands are the interface layer 3 IGMP commands for the switch.

The `config ip l3-igmp info` command displays information about the current global layer 3 IGMP configuration.

config ip l3-igmp interface Commands

The `config ip l3-igmp interface` commands allow you to configure the interface IP address `<ipaddr>` and use the following syntax and parameters:

config ip l3-igmp interface <ipaddr> followed by:	
`info`	Displays the settings of the IGMP interface.
`[admin-version <integer>]`	Sets the IGMP version that is supported on the router. • <integer> is 1 or 2, with a default of 2.
`last-memb-query-int <seconds>`	Sets the length of time (in seconds) an entry will remain in the multicast table before timeout. • `<seconds>` is the range of 1 to 255 with a default value of 1.
`query-interval <seconds>`	Sets the frequency (in seconds) at which host query packets are transmitted on the interface. • `<seconds>` is the range of 1 to 65535 with a default of 125.
`query-max-resp <integer>`	Sets the maximum response time (in seconds) advertised in IGMPv2 queries on the interface. Smaller values allow a router to prune groups faster. • `<seconds>` is the range of 1 to 255 with a default of 10.
`robustval <integer>`	Allows tuning for the expected packet loss of a network. • `<seconds>` is the range of 2 to 255 with a default of 2. Increase the value if you expect the network to experience some packet loss.
`[version <integer>]`	Sets the version of IGMP that is running on the interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is IGMPv2. • `<integer>` is 1 or 2, with a default of 2.

show ip l3-igmp Commands

These commands display information about IGMP on the switch.

show ip l3-igmp cache Command

The `show ip l3-igmp cache` command displays information about the layer 3 IGMP cache.

The command uses the syntax:

```
show ip l3-igmp cache
```

Figure 5-14 is a sample output.

```
Passport-8610/show/ip/l3-igmp# cache

================================================================================
                                    Igmp Cache
================================================================================
GRPADDR         INTERFACE  LASTREPORTER    EXPIRATION V1HOSTTIMER
--------------------------------------------------------------------------------
225.1.2.5       Vlan52     192.28.1.8      131        0
```

Figure 5-14. *show ip l3-igmp cache* Command Output

show ip l3-igmp group Command

The `show ip l3-igmp group` command displays information for the layer 3 IGMP group.

The command uses the syntax:

```
show ip l3-igmp group
```

Figure 5-15 is a sample output.

```
Passport-8610/show/ip/l3-igmp# group

================================================================================
                                    Igmp Group
================================================================================
GRPADDR         INPORT     MEMBER          EXPIRATION
--------------------------------------------------------------------------------
225.1.2.5       cpp        192.28.1.8      169
```

Figure 5-15. *show ip l3-igmp group* Command Output

show ip l3-igmp interface Command

The `show ip l3-igmp interface` command displays the following information for the interfaces on which layer 3 IGMP is enabled.

The command uses the syntax:

```
show ip l3-igmp interface
```

Figure 5-16 is a sample output.

```
Passport-8610/show/ip/l3-igmp# interface

================================================================================
                                    Igmp Interface
================================================================================
        QUERY                                QUERY   WRONG               LASTMEM
IF      INTVL STATUS VERS. QUERIER           MAXRSPT QUERY JOINS ROBUST  QUERY
--------------------------------------------------------------------------------
P7/1    125   inact  2     0.0.0.0           10      0     0     2       1
V2      125   inact  2     0.0.0.0           10      0     0     2       1
V3      125   inact  2     0.0.0.0           10      0     0     2       1
V4      125   inact  2     0.0.0.0           10      0     0     2       1
V5      125   inact  2     0.0.0.0           10      0     0     2       1
V6      125   inact  2     0.0.0.0           10      0     0     2       1
V10     125   inact  2     0.0.0.0           10      0     0     2       1
V15     125   inact  2     0.0.0.0           10      0     0     2       1
V18     125   inact  2     0.0.0.0           10      0     0     2       1
V23     125   inact  2     0.0.0.0           10      0     0     2       1
V27     125   inact  2     0.0.0.0           10      0     0     2       1
V51     125   inact  2     0.0.0.0           10      0     0     2       1
V52     125   active 2     192.28.1.20       10      0     1     2       1
```

Figure 5-16. *show ip l3-igmp interface* Command Output

config ethernet <ports> ip l3-igmp Commands

The `config ethernet <ports> ip l3-igmp` commands allow you to configure layer 3 IGMP on the specified port(s). The commands require the parameter `<ports>` as the port or list of ports {slot/port[-slot/port][, ...]}.

config ethernet <ports> ip l3-igmp followed by:	
`info`	Displays IGMP settings on the port.
`last-memb-query-int <seconds>`	Sets the length of time (in seconds) an entry will remain in the multicast table before timeout. • `<seconds>` is the range of 1 to 255 with a default value of 1.
`query-interval <seconds>`	Sets the frequency (in seconds) at which host query packets are transmitted on the port. • `<seconds>` is the range is 1 to 65535 with a default of 125.
`query-max-resp <seconds>`	Sets the maximum response time (in seconds) advertised in IGMPv2 queries on the port. Smaller values allow a router to prune groups faster. • `<seconds>` is the range of 1 to 255 with a default of 10.
`robustval <integer>`	Allows tuning for the expected packet loss of a network. • `<seconds>` is the range of 2 to 255 with a default of 2. Increase the value if you expect the network to experience packet loss.
`version <integer>`	Sets the version (1 or 2) of IGMP that is running on the port. For IGMP to function correctly, all routers on a LAN must use the same version. • `<integer>` is 1 or 2, with a default of 2.

Figure 5-17 shows a sample of the `config ethernet <ports> ip l3-igmp info` command.

```
Passport-8610# config ethernet 9/2 ip l3-igmp info

Sub-Context:
Current Context:

         last-memb-query-int : 1
              query-interval : 125
              query-max-resp : 10
                   robustval : 2
                     version : 2
```

Figure 5-17. *config ethernet ip l3-igmp info* Command Output

show ports info l3-igmp Command

The `show ports info l3-igmp` command displays IGMP information about the specified port or for all ports.

The command uses the syntax:

`show ports info l3-igmp [<ports>]`

Figure 5-18 is a sample display.

```
Passport-8610# show ports info l3-igmp

================================================================================
                                    Port Ip Igmp
================================================================================
PORT_NUM QUERY_INTERVAL  QUERY_MAX_RESP  ROBUST     VERSION    LSTMEMBER_QUERY
--------------------------------------------------------------------------------
9/1      125             10              2          version2   1
9/2      125             10              2          version2   1
9/3      125             10              2          version2   1
9/4      125             10              2          version2   1
9/5      125             10              2          version2   1
9/6      125             10              2          version2   1
9/7      125             10              2          version2   1
9/8      125             10              2          version2   1
```

Figure 5-18. *show ports info 13-igmp* Command (Partial Output)

config vlan <vid> ip l3-igmp Commands

The `config vlan <vid> ip l3-igmp` commands allow you to configure layer 3 IGMP on the VLAN, where VLAN ID `<vid>` is from 1 to 4094. The commands use the following syntax and parameters:

config vlan <vid> ip l3-igmp followed by:	
`info`	Displays IGMP settings on the VLAN.
`last-memb-query-int <seconds>`	Sets the length of time (in seconds) an entry will remain in the multicast table before timeout. • `<seconds>` is the range of 1 to 255 with a default value of 1.
`query-interval <seconds>`	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. • `<seconds>` is the range of 1 to 65535 with a default of 125.
`query-max-resp <seconds>`	Sets the maximum response time (in seconds) advertised in IGMPv2 queries on the VLAN. Smaller values allow a router to prune groups faster. • `<seconds>` is the range of 1 to 255 with a default of 10.
`robustval <integer>`	Allows tuning for the expected packet loss of a network. • `<seconds>` is the range of 2 to 255 with a default of 2. Increase the value if you expect the network to experience loss.
`version <integer>`	Sets the version (1 or 2) of IGMP that is running on the VLAN. For IGMP to function correctly, all routers on a LAN must use the same version. • `<integer>` is either 1 or 2 with a default of 2.

Figure 5-19 shows a sample of the `config vlan ip l3-igmp info` command.

```
Passport-8610# config vlan 1 ip l3-igmp info

Sub-Context:
Current Context:

         last-memb-query-int : 1
              query-interval : 125
              query-max-resp : 10
                   robustval : 2
                     version : 2
```

Figure 5-19. *config vlan ip l3-igmp info* Command Output

show vlan info l3-igmp Command

The `show vlan info l3-igmp` command displays the IGMP configuration for all VLANs on the switch or for the specified VLAN.

The command uses the syntax:

```
show vlan info l3-igmp [<vid>]
```

Figure 5-20 is a sample display.

```
Passport-8610# show vlan info l3-igmp

================================================================================
                                    Vlan Ip Igmp
================================================================================
VLAN_ID  QUERY_INTERVAL  QUERY_MAX_RESP  ROBUST     VERSION    LSTMEMBER_QUERY
--------------------------------------------------------------------------------
1        125             10              2          version2   1
```

Figure 5-20. *show vlan info l3-igmp* Command Output

Chapter 6
IPX Commands

This chapter describes the Run-Time CLI IPX commands that are used in the Passport 8000 Series switch.

IPX Commands

This section provides information about using the Passport CLI for configuring and displaying the Internet Packet Exchange (IPX) protocol, the Novell Inc. adaptation of the Xerox Network System (XNS) protocol.

The Passport implementation of IPX supports four Ethernet frame formats:

- Ethernet II (ipxEthernet2)
- 802.2-LLC (ipx802dot2)
- 802.3-RAW (ipx802dot3)
- 802.3-SNAP (ipxSnap)

In addition to the IPX configuration commands, there are also commands for IPX RIP and IPX SAP.

config ipx Commands

The IPX commands allow you to configure an IPX interface on the switch.

To configure an IPX interface:

1. **Create a protocol-based VLAN, using one of the four supported Ethernet frame formats.**

   ```
   config vlan <vid> create byprotocol <sid>
   <ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2> [name <value>]
   [color <value>]
   ```

   where:

   `vid` is the VLAN ID (2 to 4094).
   `sid` is the spanning tree ID (1 to 25).
   `protocol` is one of the four listed above.
   `name <value>` is the name of the VLAN, for example IPX.
   `color <value>` is the color of the VLAN (0 to 32).

Note: You can also create a port-based VLAN in IPX. The procedure is the same as for a protocol-based VLAN except that you do not need to assign an encapsulation method when you create the VLAN. Use the command:
`config vlan <vid> create byport <sid> [name <value>]`

2. **Remove the ports that you do not want to be part of the interface:**

   ```
   config vlan <vid> ports remove <ports> [member <value>]
   ```

   where:

   `vid` is the VLAN created in step 1.

   `member <value>` is the slot and port number to be removed from the interface (for example, 1/5-1/16).

3. **Add the ports that you do want to be part of the interface:**

   ```
   config vlan <vid> ports add <ports> [member <value>]
   ```

   where:

   `vid` is the VLAN created in step 1.

   `member <value>` is the slot and port number to be added to the interface (for example, 1/1-1/4).

4. **Create an IPX network interface with the specified VLAN ID and encapsulation method.**

   ```
   config vlan <vid> ipx create <IPX-network-number>
   [<encapsulation>]
   ```

   where:

   `vid` is the VLAN created in step 1.

   `encapsulation` is ethernet-ii, snap, llc, or raw.

Note: The encapsulation method must be the same as the protocol selected in step 1.

5. **Globally enable IPX routing on all IPX interfaces:**

   ```
   config ipx forwarding enable
   ```

The `config ipx` commands use the following syntax and parameters:

`config ipx` `followed by:`	
`info`	Displays the switch IPX configuration.
`forwarding info`	Indicates whether IPX is enabled or disabled on the switch and lists the IPX networks that are enabled or disabled.
`forwarding disable [<IPX-network-number>]`	Disables IPX forwarding globally or on the specified IPX network.
`forwarding enable [<IPX-network-number>]`	Enables IPX forwarding globally or on the specified IPX network.

config vlan <vid> ipx Commands

The `config vlan ipx` commands allow you to configure IPX on a VLAN using the following syntax and commands:

config vlan <vid> ipx followed by:	
`info`	Displays the switch IPX configuration.
`create <IPX-network-number> [<encapsulation>]`	Creates a protocol-based VLAN using one of the supported encapsulation methods as the protocol: • `<IPX-network-number>` is the destination IPX network number for the route. • `<encapsulation>` is <ipx802dot3 | ipx802dot2 | ipxSnap | pxEthernet2>.
`delete <IPX-network-number>`	Deletes the specified IPX network.

config ipx set Commands

The `config ipx set` commands allow you to configure maximum entries for IPX parameters and to use the following syntax:

config ipx set followed by:	
`info`	Displays current maximum entries set on the switch.
`max-route <max_entries>`	Used to set the maximum number of IPX routes that can be learned by the switch. **Note**: To take effect, save the configuration and reset the switch.
`max-sap <max_entries>`	Used to set the maximum number of IPX services that can be learned by the switch. **Note**: To take effect, save the configuration and reset the switch.
`max-static-route <max_entries>`	Used to set the maximum number of static IPX routes that can be configured on the switch. **Note**: To take effect, save the configuration and reset the switch.

config ipx set followed by:	
max-static-sap <max_entries>	Used to set the maximum number of static IPX services that can be configured on the switch. **Note**: To take effect, save the configuration and reset the switch.
netbios <on|off>	Turns on or off IPX NetBIOS (type 20) propagation on all the switch's IPX interfaces. **Note:** Nortel Networks recommends that you disable IPX NetBIOS only temporarily, possibly for trouble shooting; otherwise, a broadcast loop will be cut.

Figure 6-1 shows a sample of the `config ipx set info` command.

```
Passport-8610# config ipx set info
                    max-route - 1500
                      max-sap - 1500
              max-static-route - 128
                max-static-sap - 64
```

Figure 6-1. *config ipx set info* Command Output

config ipx static-route Commands

The `config ipx static-route` commands allow you to create or delete a static IPX network route.

The commands use the following syntax and parameters:

config ipx static-route followed by:	
`info`	Displays IPX routes created and/or deleted.
`create <IPX-network-number> <nexthop> <hop-count> <tick-count>`	Creates a static IPX network route where: • `<nexthop>` is the IPX address of the next router. • `<hop-count>` is the number of passes through a router. • `<tick-count>` is the number of ticks (1/18th of a second). To create a default route, enter FF:FF:FF:FE as the IPX network number.
`delete <IPX-network-number>`	Deletes the static IPX network route.

Figure 6-2 shows a sample of the `config ipx static-route info` command.

```
Passport-8610# config ipx static-route info

Sub-Context:
Current Context:

              create :
              delete : N/A
```

Figure 6-2. *config ipx static-route info* Command Output

config ipx rip Commands

These commands allow you to configure Routing Information Protocol (RIP) on IPX interfaces. Three timing parameters (hold-multiplier, delay-timer, and interval-timer) control IPX RIP behavior. If you do not use the factory defaults and change global default parameters, you should set the global parameters prior to setting individual interface parameters.

config ipx rip info Command

The `config ipx rip info` command displays IPX RIP settings on the switch.

The command uses the syntax:

```
config ipx rip info
```

config ipx rip default Commands

The `config ipx rip default` commands allow you to set the IPX RIP default values using the following syntax and parameters:

config ipx rip followed by:	
`default-delay <delay-timer>`	Sets the delay timer default values in milliseconds. • `<delay-timer>` is the range of 1 to 1000 with the default of 50 ms.
`default-hold-multiplier <hold-multiplier>`	Sets the hold multiplier default value. • `<hold-multiplier>` is the range of 1 to 2147483647 with the default of 3.
`default-interval <interval-timer>`	Sets the interval timer default values in seconds. • `<interval-timer>` is the range of 1 to 2147483647 with the default of 60 seconds.

config ipx rip Commands

The `config ipx rip` commands allow you to set the IPX RIP interface values, and require an IPX network number `<IPX-network-number>`.

config ipx rip followed by:	
`hold-multiplier <IPX-network-number> <hold-multiplier>`	Sets the hold multiplier value for the IPX interface. • `<hold-multiplier>` is the range of 1 to 2147483647 with the default of 3.
`update-delay <IPX-network-number> <delay-timer>`	Sets the update delay timer for the IPX interface. • `<delay-timer>` is the range of 1 to 1000 ms with the default of 50 ms.
`update-interval <IPX-network-number> <interval-timer>`	Sets the update interval for the IPX interface in seconds. • `<interval-timer>` is the range of 1 to 2147483647 with the default of 60 seconds.

config ipx sap Commands

The IPX SAP commands allow you to configure Service Advertisement Protocol (SAP) on IPX interfaces. Three timing parameters (hold-multiplier, delay-timer, and interval-timer) also control IPX SAP behavior. If you do not use the factory defaults and change global default parameters, you should set the global parameters prior to setting individual interface parameters.

config ipx sap info Command

The `config ipx sap info` command displays IPX SAP settings on the switch.

config ipx sap default Commands

The `config ipx sap default` commands allow you to set the global default values using the following syntax and parameters:

config ipx sap followed by:	
`default-delay <delay-timer>`	Sets the delay timer default values in milliseconds. • `<delay-timer>` is a number between 1 and 1000 with the default of 50 ms.
`default-hold-multiplier <hold-multiplier>`	Sets the hold multiplier default value. • `<hold-multiplier>` is a number between 1 and 2147483647 with a default of 3.
`default-interval <interval-timer>`	Sets the interval timer default values in seconds. • `<interval-timer>` is a number between 1 and 2147483647 with a default of 60 seconds.

config ipx sap Commands

The `config ipx sap` commands allow you to set the IPX SAP parameters on the switch using the following syntax and parameters:

config ipx sap followed by:	
`create <service-type> <service-name> <ipxhost> <socket-number> <hop-count>`	Creates a static SAP entry where: • `<service-type>` is an integer between 1 and 65535. Some well-known service examples are: 0000h = unknown 0003h = print queue 0004h = file server 0005h = job server 0007h = print server 0009h = archive server 0024h = remote bridge server 0047h = advertising print server • `<service-name>` is a character string (1 to 47 characters). • `<ipxhost>` is the network and node network = IPX network number between 1 and 2147483647 node = xx:yy:zz:uu:vv:ww, where xx, yy, zz, uu, yy, and ww are 2-digit hexadecimal numbers. • `<socket-number>` is a number between 0 and 65535. • `<hop-count>` is a number between 1 and 15.
`delete <service-name>`	Deletes a static SAP entry.
`hold-multiplier <IPX-network-number> <hold-multiplier>`	Sets the hold multiplier value for the IPX interface. • `<IPX-network-number>` is the IPX network number {0x00:0x00:0x00:0x00}. • `<hold-multiplier>` is a number between 1 and 2147483647 with a default of 3.
`update-delay <IPX-network-number> <delay-timer>`	Sets the update delay timer for the IPX interface. • `<IPX-network-number>` is the IPX network number {0x00:0x00:0x00:0x00}. • `<delay-timer>` is a number between 1 and 1000 with the default of 50 ms.
`update-interval <IPX-network-number> <interval-timer>`	Sets the update interval for the IPX interface in seconds. • `<IPX-network-number>` is the IPX network number {0x00:0x00:0x00:0x00}. • `<interval-timer>` is a number between 1 to 2147483647 with the default of 60 seconds.

show ipx Commands

These commands display the configuration of IPX on the switch.

show ipx config Command

The `show ipx config` command displays general IPX configuration information for the switch or for a specified IPX network number.

The command uses the syntax:

```
show ipx config [<IPX-network-number>]
```

Figure 6-3 is a sample output.

```
Passport-8610/show/ipx# config

================================================================================
                                      Ipx Config
================================================================================
CID NETNUM     ENCAPSULATION   RIP STATUS   UPD HLD DLY SAP STATUS   UPD HLD DLY
--------------------------------------------------------------------------------
  1 0x00004444 LLC             RIP Enabled   60   3  20 SAP Enabled   60   3  20
  2 0x00005555 SNAP            RIP Enabled   60   3  20 SAP Enabled   60   3  20
```

Figure 6-3. *show ipx config* Command Output

show ipx default Command

The `show ipx default` command displays the current IPX RIP and SAP timer default values on the switch.

The command uses the syntax:

```
show ipx default
```

Figure 6-4 is a sample display.

```
Passport-8610/show/ipx# default

================================================================================
                                        Ipx Default Values
================================================================================
RIP Hold-Multiplier: 3
RIP Delay-Timer:     50 msec (20 per sec)
RIP Update-Timer:    60 sec
SAP Hold-Multiplier: 3
SAP Delay-Timer:     50 msec (20 per sec)
SAP Update-Timer:    60 sec
```

Figure 6-4. *show ipx default* Command Output

show ipx route Command

The `show ipx route` command displays information about the IPX route(s) on the switch or a specific IPX route, including the type, hop count, and ticks.

The command syntax is:

```
show ipx route [<IPX-network-number>] [<IPX-network-number>]
```

Figure 6-5 is a sample output.

```
Passport-8610/show/ipx# route

================================================================================
                                    Ipx Route
================================================================================
IPX_NET  NEXT_HOP                    TYPE   HOPS  TICS  PORT TTL
--------------------------------------------------------------------------------
00004444 00004444.00:80:2d:23:02:00 Local  1         1
00005555 00005555.00:80:2d:23:02:01 Local  1         1
00008888 00004444.00:80:2d:23:02:00 Static 1         2  cpp
```

```
3 out of 3 routes displayed.
```

Figure 6-5. *show ipx route* Command Output

show ipx sap Command

The `show ipx sap` command displays information about IPX SAP on the switch for all SAP services or a specified service.

The command uses the syntax:

```
show ipx sap [<service-name>]
```

Figure 6-6 is a sample display.

```
Passport-8610# show ipx sap

================================================================================
                                      Ipx Sap
================================================================================
SERVICE TYPE IPX HOST                 SOCKET NAME
--------------------------------------------------------------------------------
Dynamic 0004 357d72f7.00:00:00:00:00:01 0451 FTL_NS1
Dynamic 026b 357d72f7.00:00:00:00:00:01 0005 BAYNETWORKS_____________________\x9
a\xf5\xc4\xa0O@@@@@D\x85PJ
Dynamic 0278 357d72f7.00:00:00:00:00:01 4006 BAYNETWORKS_____________________\x9
a\xf5\xc4\xa0O@@@@@D\x85PJ

3 out of 3 routes displayed
```

Figure 6-6. *show ipx sap* Command Output

show ipx stats Command

The `show ipx stats` command displays IPX statistics for the specified IPX network number.

The command uses the syntax:

```
show ipx stats <IPX-network-number>
```

Figure 6-7 is a sample output.

```
Passport-8610/show/ipx# stats 0x4444
CIRCUIT_ID     NETNUM     RIP_TX     RIP_RX     SAP_TX     SAP_RX
1          0x00004444         15          0         13          0
2          0x00005555         15          0         13          0

----------------------------Total---------------------------------
                              30          0         26          0

Bad checksum         0
Received packet      550
Too many hops        0
Header error         0
Unknown socket       0
Input discard        0
Forward packet       210
Output request       508
Output no route      0
Malformed request    0
Output discard       0
Output packet        508
Resource failure     0
Bad rip              0
Bad sap              0
```

Figure 6-7. *show ipx stats* Command Output

show vlan info ipx Command

The `show vlan info ipx` command displays VLAN IPX information for the specified VLAN or all VLANs on the switch.

The command's syntax is:

```
show vlan info ipx [<vid>]
```

Figure 6-8 displays the headings for the `show vlan info ipx` command.

```
Passport-8610# show vlan info ipx

================================================================================
                                       Vlan Ipx
================================================================================
VLAN-ID VLAN-TYPE      IPXNET     ENCAPSULATION  ROUTING
--------------------------------------------------------------------------------
```

Figure 6-8. *show vlan info* Command Output

Chapter 7
Policies Commands

This chapter describes the Run-Time CLI commands that are used to configure IP policies in the Passport 8000 Series switch.

IP Policies

The `ip policy` commands allow you to configure and view IP policy features supported on a Passport switch. The accept and announce policies are configured for the switch according to the selected protocol (RIP or OSPF). A policy is made up of three parts: matching criteria, set parameters, and action. The matching criteria are used to decide whether or not a policy should be applied to a certain route.

After an announce policy is selected for a route, the set parameters construct the route advertisement only if the action is announce. After an accept policy is selected for a route, the set parameters are used to introduce the route into the routing table if the action is to accept.

config ip policy Commands

There are several basic categories of IP policy commands:

- `config ip policy info` command
- `config ip policy addrlist` commands
- `config ip policy netlist` commands
- `config ip policy ospf` commands
- `config ip policy ospf accept` commands
- `config ip policy ospf announce` commands
- `config ip policy rip` commands

- `config ip policy rip accept` commands
- `config ip policy rip announce` commands

config ip policy addrlist Commands

The `config ip policy addrlist` commands allow you to set address list matching criteria to suit a given route. The parameter `<listid>` is the address list ID (1 to 1000).

The commands use the following syntax and parameters:

config ip policy addrlist <listid> followed by:	
`info`	Displays the address list characteristics.
`add-address <ipaddr>`	Adds an IP address to the policy address list.
`create`	Creates a policy address list.
`delete`	Deletes the policy address list.
`name <name>`	Assigns a name to the policy address list.
`remove-address <ipaddr>`	Removes an address from the policy address list.

Figure 7-1 shows an example of the `config ip policy addrlist info` command.

```
Passport-8610# config ip policy addrlist 1 info

Sub-Context:
Current Context:

                     create :
                     delete : N/A
                       name : ADDRLIST#1
                add-address :
             remove-address : N/A
```

Figure 7-1. *config ip policy addrlist info* Command Output

config ip policy netlist Commands

The `config ip policy netlist` commands allow you to set network list matching criteria to suit a given route where `<listid>` is the network list ID (1 to 1000).

The commands use the following syntax and parameters:

config ip policy netlist <listid> followed by:	
`info`	Displays settings for the IP policy network list.
`add-network <ipaddr/mask>`	Adds a network with the IP address and subnet mask to the policy network list.
`create`	Creates a policy network list.
`delete`	Deletes the policy network list.
`name <name>`	Assigns a name to the policy network list.
`remove-network <ipaddr/mask>`	Removes an address from the policy address list.

Figure 7-2 shows an example of the `config ip policy netlist info` command.

```
Passport-8610# config ip policy netlist 3 info

Sub-Context:
Current Context:

                     create :
                     delete : N/A
                       name : NETLIST#3
                 add-network :
              remove-network : N/A
```

Figure 7-2. *config ip policy netlist info* Command Output

config ip policy ospf Commands

The `config ip policy ospf` commands allow you to globally apply the configured OSPF accept or announce policies to the switch. After you have set up OSPF policies, you must apply the policies before they take effect.

config ip policy ospf followed by:	
`info`	Displays global status of OSPF accept and announce policies.
`apply-accept`	Globally applies OSPF accept policies to the switch.
`apply-announce`	Globally applies OSPF announce policies to the switch.

Note: Although individual policies may be configured and enabled, they will not take effect until the global apply command is issued.

config ip policy ospf accept Commands

The `config ip policy ospf accept` commands allow you to configure the OSPF accept policy with a policy ID `<pid>` range from 6001 to 7000.

The commands use the following syntax and parameters:

config ip policy ospf accept <pid> followed by:	
`info`	Displays the current OSPF accept policy settings.
`action <accept|ignore>`	Selects whether the OSPF policy action will be to accept or ignore external route information.
`create`	Creates an OSPF accept policy.
`delete`	Deletes an OSPF accept policy.
`disable`	Disables an OSPF accept policy.
`enable`	Enables an OSPF accept policy.

config ip policy ospf accept <pid> followed by:	
exact-net-list <netlist id>	Sets an OSPF accept policy in which networks will only match the specific network advertisement. • <netlist id> is the netlist id range 0 to 1000.
ext-metric-type <type1|type2>	Sets the OSPF accept policy external metric type to type 1 or type 2.
inject-net-list <netlist id>	Sets an OSPF accept policy that will insert networks into the routing table that differ from the actual advertised network. • <netlist id> is the netlist id range 0 to 1000.
name <string>	Assigns the OSPF accept policy name.
precedence <precedence>	Sets the precedence for the OSPF accept policy. • <precedence> is the range 0 to 65535. If multiple policies apply, the higher precedence is used.
range-net-list <netlist id>	Sets the OSPF accept policy to match any network number that falls into the indicated range. • <netlist id> is the netlist id range 0 to 1000.

Figure 7-3 shows an example of `config ip policy ospf accept info` command.

```
Passport-8610/config/ip/policy/ospf# accept 6003 info

Sub-Context: accept announce
Current Context:

                     action : accept
                     create :
                     delete : N/A
                     enable : true
              exact-net-list : 0
             ext-metric-type : any
          inject-net-list-id : 0
                       name : POLICY-6003
                 precedence : 0
           range-net-list-id : 0
```

Figure 7-3. *config ip policy ospf accept info* Command Output

config ip policy ospf announce Commands

The `config ip policy ospf announce` commands allow you to configure the OSPF announce policy, where the OSPF announce policy ID `<pid>` is in the range 2001 to 3000.

The commands use the following syntax and parameters:

config ip policy ospf announce <pid> followed by:	
`info`	Displays the settings for the OSPF announce policy.
`action <accept|ignore>`	Selects whether the OSPF policy action will be to accept or ignore external route information.
`add-route-source <direct|static|rip|any>`	Adds a route source to the announce policy; sets direct, static, RIP, or any as accepted sources from which the route can be learned.
`advertise-netlist <netlist id>`	If the action is set to announce, allows sending or advertising networks that differ from the actual network in the routing table. • `<netlist id>` is the netlist id range 0 to 1000 and allows advertisement of an aggregate or default along with the actual network.
`create`	Creates an OSPF announce policy.
`delete`	Deletes an OSPF announce policy.
`disable`	Disables an OSPF announce policy.
`enable`	Enables an OSPF announce policy.
`exact-netlist <netlist id>`	Sets an OSPF announce policy in which networks will only match the specific network advertisement. • `<netlist id>` is the netlist id range 0 to 1000.
`ext-metric <ext-metric>`	Sets the OSPF announce external metric (0 to 65535).
`ext-metric-type <type1|type2>`	Sets the OSPF announce policy external metric type to type 1 or type 2.
`name <string>`	Assigns the OSPF announce policy name.
`precedence <precedence>`	Sets the precedence for the OSPF announce policy. The range is 0 to 65535. If multiple policies apply, the higher precedence is used.
`range-netlist <netlist id>`	Sets the OSPF announce policy to match any network number that falls into the indicated range. • `<netlist id>` is the netlist id range 0 to 1000.

config ip policy ospf announce <pid> followed by:	
remove-route-source <direct|static|rip|any>	Removes a route source from the announce policy.
rip-gateway-list <addrlist id>	Identifies the RIP gateway lists that are associated with this announce policy. • <addrlist id> is the RIP gateway list ID (0 to 1000) and applies only to RIP sourced routes if RIP is included as a route source.
rip-interface-list <addrlist id>	Indicates the entries in the RIP interface lists that are associated with this announce policy. • <addrlist id> is the RIP interface list ID (0 to 1000) and applies only to RIP sourced routes if RIP is included as a route source.

Figure 7-4 shows an example of the `config ip policy ospf announce info` command.

```
Passport-8610/config/ip/policy/ospf# announce 2003 info

Sub-Context: accept announce
Current Context:

                    action : ignore
      add-route-source : direct|static|rip
     advertise-net-list : 0
                    create :
                    delete : N/A
                    enable : true
          exact-netlist : 0
           exact-metric : 0
       ext-metric-type : type2
                  name : POLICY-2003
            precedence : 0
          range-netlist : 0
    remove-route-source : N/A
       rip-gateway-list : 0
     rip-interface-list : 0
```

Figure 7-4. *config ip policy ospf announce info* Command Output

config ip policy rip Commands

The `config ip policy rip` commands are used to apply the configured RIP accept or announce policies to the switch. Use the `config ip policy rip info` command to display the current status.

config ip policy rip accept Commands

The `config ip policy rip accept` commands allow you to configure the RIP accept policy, where `<pid>` is the RIP accept policy ID (4001 to 5000).

The commands use the following syntax and parameters:

config ip policy rip accept <pid> followed by:	
`info`	Displays the settings for the RIP accept policy.
`action <accept|ignore>`	Selects whether the RIP policy action will be to accept or ignore matches.
`apply-mask <ipmask>`	Sets an IP subnet mask for the RIP accept policy, where `<ipmask>` is the apply-mask `{a.b.c.d}`.
`create`	Creates a RIP accept policy.
`delete`	Deletes a RIP accept policy.
`disable`	Disables a RIP accept policy.
`enable`	Enables a RIP accept policy.
`exact-netlist <netlist id>`	Sets a RIP accept policy in which networks will only match the specific network advertisement. • `<netlist id>` is the netlist id range to 1000.
`inject-netlist <netlist id>`	Sets a RIP accept policy that will insert networks into the routing table that differ from the actual advertised network. • `<netlist id>` is the netlist id range 0 to 1000.
`name <string>`	Assigns a RIP accept policy name.
`precedence <precedence>`	Sets the precedence for the RIP accept policy. The range is 0 to 65535. If multiple policies apply, the higher precedence is used.

config ip policy rip accept <pid> followed by:	
range-netlist <netlist id>	Sets the RIP accept policy to match any network number that falls into the indicated range. • <netlist id> is the netlist id range 0 to 1000.
rip-gateway-list <addrlist id>	Identifies the RIP gateway lists that are associated with this policy. • <addrlist id> is the RIP gateway list ID (0 to 1000) and applies only to RIP sourced routes if RIP is included as a route source.
rip-interface-list <listid>	Indicates the entries in the RIP interface lists that are associated with this policy. • <listid> is the RIP interface list ID (0 to 1000) and applies only to RIP sourced routes if RIP is included as a route source.

Figure 7-5 shows an example of the `config ip policy rip accept info` command.

```
Passport-8610/config/ip/policy/rip# accept 4003 info

Sub-Context: accept announce
Current Context:

                    action : accept
                apply-mask : 0.0.0.0
                    create :
                    delete : N/A
                    enable : true
            exact-net-list : 0
           inject-net-list : 0
                      name : POLICY-4003
            range-net-list : 0
          rip-gateway-list : 0
       rip-interface-list : 0
              precedence : 0
```

Figure 7-5. *config ip policy rip accept info* Command Output

config ip policy rip announce Commands

The `config ip policy rip announce` commands allow you to configure the RIP announce policy, where `<pid>` is the RIP announce policy ID (1 to 1000).

The commands use the following syntax and parameters:

config ip policy rip announce <pid> followed by:	
`info`	Displays the settings for the RIP announce policy.
`action <accept|ignore>`	Selects whether the RIP policy action will be to accept or ignore matches.
`add-route-source <direct|static|rip|ospf|any>`	Adds a route source to the announce policy.
`advertise-netlist <netlist id>`	If the action is set to announce, allows sending or advertising networks that differ from the actual network in the routing table advertise network list. • `<netlist id>` is the netlist id range 0 to 1000.
`create`	Creates a RIP announce policy.
`delete`	Deletes a RIP announce policy.
`disable`	Disables a RIP announce policy.
`enable`	Enables a RIP announce policy.
`exact-netlist <netlist id>`	Sets a RIP announce policy exact network list. • `<netlist id>` is the netlist id range 0 to 1000.
`name <string>`	Assigns a RIP accept policy name.
`ospf-router-id-list <addrlist id>`	Indicates the entries in the OSPF router lists that are associated with this policy. • `<addrlist id>` is OSPF router-id list {0..1000} . It is valid only for OSPF-routed sourced routes if OSPF is included as a route source.
`ospf-route-type <type1|type2|external|internal|any>`	Indicates the entries in the OSPF router lists that are associated with this policy: type 1, type 2, external routes, internal routes, or any OSPF routes.

config ip policy rip announce <pid> followed by:	
outbound-interface-list <addrlist id>	Indicates the entries in the outbound lists that are associated with this policy. • <addrlist id> is OSPF router-id list {0..1000}.
precedence <precedence>	Sets the precedence for the RIP announce policy. • <precedence> is the range is 0 to 65535. If multiple policies apply, the higher precedence is used.
range-netlist <netlist id>	Sets the RIP announce policy to match any network number that falls into the indicated range. • <netlist id> is the range from 0 to 1000.
remove-route-source <direct|static|rip|ospf|any>	Removes a route source from the announce policy.
rip-gateway-list <addrlist id>	Identifies the RIP gateway lists that are associated with this policy. The RIP gateway list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.
rip-interface-list <listid>	Indicates the entries in the RIP interface lists that are associated with this policy. The RIP interface list ID (0 to 1000) applies only to RIP sourced routes if RIP is included as a route source.
rip-metric <rip-metric>	Sets the RIP external metric (0 to 15) for the policy, the external metric to use when advertising a route that matches this policy. Meaningful only if the set action is announce.

Figure 7-6 shows the `config ip policy rip announce info` command.

```
Passport-8610/config/ip/policy/rip# announce 3 info

Sub-Context: accept announce
Current Context:

                      action : ignore
           add-route-source : direct|static|rip|ospf
         advertise-net-list : 3
                      create :
                      delete : N/A
                      enable : true
              exact-net-list : 0
                        name : POLICY-3
           ospf-router-list : 0
            ospf-route-type : any
 outbound-interface-list : 0
                  precedence : 0
             range-net-list : 0
        remove-route-source : N/A
           rip-gateway-list : 0
          rip-interface-list : 0
                  rip-metric : 0
```

Figure 7-6. *config ip policy rip announce info* Command Output

show ip policy Commands

The following commands provide information about the IP policies that are set up on the switch.

show ip policy addrlist info Command

The `show ip policy addrlist info` command displays the IP policy address lists set on the switch. If no address list ID is entered, all address lists on the switch are listed.

This command uses the syntax:

```
show ip policy addrlist info [id <value>]
```

Figure 7-7 is a sample.

```
Passport-8606# show ip policy addrlist info

================================================================================
                                      Policy AddrList
================================================================================
ID   NAME
--------------------------------------------------------------------------------
1    ADDRLIST#1
```

Figure 7-7. *show ip policy addrlist info* Command Output

show ip policy netlist info Command

The `show ip policy netlist info` command displays the network lists configured on the switch. If no ID is entered, information is displayed about all network lists on the switch.

This command uses the syntax:

```
show ip policy netlist info [id <value>]
```

Figure 7-8 is an example.

```
Passport-8606# show ip policy netlist info

================================================================================
                                     Policy NetList
================================================================================
ID   NAME
--------------------------------------------------------------------------------
3    NETLIST#3
```

Figure 7-8. *show ip policy netlist info* Command Output

show ip policy ospf accept info Command

The `show ip policy ospf accept info` command displays information about the OSPF accept policies configured on the switch. If a policy ID is entered, the display lists information for only that policy.

This command uses the syntax:

```
show ip policy ospf accept info [id <value>]
```

Figure 7-9 is an example.

```
Passport-8606# show ip policy ospf accept info

================================================================================
                                    Policy Ospf Accept Info
================================================================================
PID  NAME                           ENABLE PREC  ACTION   OSPFTYPE
--------------------------------------------------------------------------------
6003 POLICY-6003                    true   0     accept   any
```

Figure 7-9. *show ip policy ospf accept info* Command Output

show ip policy ospf accept lists Command

The `show ip policy ospf accept lists` command displays the accept lists on the switch. If an ID is entered, only that list is displayed.

This command uses the syntax:

```
show ip policy ospf accept lists [id <value>]
```

Figure 7-10 is a sample.

```
Passport-8606# show ip policy ospf accept lists

================================================================================
                                    Policy Ospf Accept List
================================================================================
POLICY_ID       EXACTNETLIST    RANGENETLIST    INJECTNETLIST
--------------------------------------------------------------------------------
6003            0               0               0
```

Figure 7-10. *show ip policy ospf accept lists* Command Output

show ip policy ospf accept match network Command

The `show ip policy ospf accept match network` command lists the policies that match the specified network with a range or exact match.

This command uses the syntax:

```
show ip policy ospf accept match network <value>
```

The format is the same as the command for a RIP accept policy displayed in Figure 7-15 on page 7-17.

show ip policy ospf announce info Command

The `show ip policy ospf announce info` command displays information about the OSFP announce policies configured on the switch. If a policy ID is entered, the display lists information for only that policy.

This command uses the format:

```
show ip policy ospf announce info [id <value>]
```

Figure 7-11 is a sample.

```
Passport-8610# show ip policy ospf announce info

================================================================================
                                  Policy Ospf Announce Info
================================================================================
PID  NAME                          ENABLE PREC  RTSRC  ACTION   TYPE     MTRC
--------------------------------------------------------------------------------
2003 POLICY-2003                   true   0     direct|static|rip ignore   ty
pe2    0
```

Figure 7-11. *show ip policy ospf announce info* Command Output

show ip policy ospf announce lists Command

The `show ip policy ospf announce lists` command displays list characteristics of the OSPF announce policies configured on the switch or for a specified policy ID.

The syntax is:

```
show ip policy ospf announce lists [id <value>]
```

Figure 7-12 is a sample.

```
Passport-8610# show ip policy ospf announce lists

================================================================================
                                    Policy Ospf Announce List
================================================================================
POLICY_ID  EXACTNETLIST RANGENETLIST ADVERNETLIST RIPGATELIST  RIPINTERLIST
--------------------------------------------------------------------------------
2003       0            0            0            0            0
```

Figure 7-12. *show ip policy ospf announce lists* Command Output

show ip policy ospf announce match network Command

The `show ip policy ospf announce match network` command lists the policies that match the specified network with a range or exact match.

This command uses the syntax:

```
show ip policy ospf announce match network <value>
```

The format is the same as the command for RIP accept policy displayed in Figure 7-15 on page 7-17.

show ip policy rip accept info Command

The `show ip policy rip accept info` command displays information about the RIP accept policies configured on the switch. If a policy ID is entered, the display lists information for only that policy.

This command is in the format:

```
show ip policy rip accept info [id <value>]
```

Figure 7-13 is a sample.

```
Passport-8610# show ip policy rip accept info

================================================================================
                                    Policy Rip Accept Info
================================================================================
PID  NAME                          ENABLE PREC  ACTION   APPLYMASK
--------------------------------------------------------------------------------
4003 POLICY-4003                   true   0     accept   0.0.0.0
```

Figure 7-13. *show ip policy rip accept info* Command Output

show ip policy rip accept lists Command

The `show ip policy rip accept lists` command displays the accept lists on the switch. If an ID is entered, only that list is displayed.

This command uses the syntax:

```
show ip policy rip accept lists [id <value>]
```

Figure 7-14 is a sample.

```
Passport-8610# show ip policy rip accept lists

================================================================================
                                    Policy Rip Accept List
================================================================================
ID         EXACTNETLIST RANGNETLIST  INJCTNETLIST RIPGATEWAY   RIPINTERFACE
--------------------------------------------------------------------------------
4003       0            0            0            0            0
```

Figure 7-14. *show ip policy rip accept lists* Command Output

show ip policy rip accept match network Command

The `show ip policy rip accept match network` command lists the policies that match the specified network with a range or exact match.

This command uses the following format, where `<value>` is the network address {a.b.c.d/x | a.b.c.d/x.x.x.x | default}:

```
show ip policy rip accept match network <value>
```

Figure 7-15 is a sample.

```
Passport-8606# show ip policy rip accept match network 4.1.1.5/255.0.0.0

================================================================================
                                  Policy Rip Accept Match Network
================================================================================
RipAccept Policy Ids: 4001
```

Figure 7-15. *show ip policy rip accept match network* Command Output

show ip policy rip announce info Command

The `show ip policy rip announce info` command displays information about RIP announce policies on the switch or about a specified RIP announce policy.

This command uses the syntax:

```
show ip policy rip announce info [id <value>]
```

The command output is similar to the OSPF announce policy displayed in Figure 7-11 on page 7-15.

show ip policy rip announce lists Command

The `show ip policy rip announce lists` command displays information about RIP announce policy lists on the switch or about a specific RIP announce policy list.

This command uses the syntax:

```
show ip policy rip-announce lists [id <value>]
```

The output is similar to the OSPF announce list table displayed in Figure 7-12 on page 7-15.

show ip policy rip announce match network Command

The `show ip policy rip announce match network` command lists the policies that match the specified network with a range or exact match.

This command uses the format:

```
show ip policy rip announce match network <value>
```

The output is similar as the output from the `show ip policy rip accept match network <value>` displayed in Figure 7-15 on page 7-17.

Chapter 8
IP QoS and Traffic Filter Commands

This chapter describes the Run-Time CLI commands that are used to configure IP QoS and IP traffic filters in the Passport 8000 Series switch. This chapter includes sections about the following command groups:

- IP QoS Commands
- IP Traffic Filters

IP QoS Commands

The IP QoS commands allow you to enable the Quality of Service (QoS) features on the switch. Refer to *Networking Concepts for the Passport 8000 Series Switch* for general information on Quality of Service features.

To enable end-to-end QoS for IP traffic, you must identify which ports will serve as the DiffServ access port(s) and which ports will serve as DiffServ core port(s) and set them accordingly.

To enable DiffServ for IP traffic:

1. **Enable DiffServ on the ports using the following command:**

   ```
   config ethernet <ports> enable-diffserv true
   ```

2. **Enable the DiffServ access ports using the following command:**

   ```
   config ethernet <ports> access-diffserv true
   ```

3. **Enable the DiffServ core ports using the following command:**

   ```
   config ethernet <ports> access-diffserv false
   ```

The Passport 8000 Series switch contains the QoS mapping needed to enable a DiffServ domain. You can view the default QoS configurations, including the following:

- The egress and ingress mapping tables for the DiffServ codepoints (DSCP) and the eight QoS levels
- The traffic classification and policing variables

To view the traffic classification and policing variables, use the following commands:

- `show qos queue`
- `config ip traffic-filter traffic-profile <pid> info`
- `config qos ingressmap info`
- `config qos egressmap info`

To view the DiffServ settings for non-IP traffic, use the following commands to display the QoS setting for VLANs, ports, and MAC addresses, respectively:

- `config vlan <vid> info`
- `config ethernet <ports> info`
- `show vlan info fdb-entry <vid>`

Caution: Nortel Networks recommends not changing the default values. If you change the values, make sure that the values are consistent on all other Passport switches and other devices in your network. Inconsistent mapping of values can result in unpredictable service levels.

config qos Commands

The `config qos` commands allow you to view IEEE 802.1p levels and DSCP bytes to QoS level maps and to change those settings, if necessary.

The `config qos` commands take the following syntax and format:

config qos followed by:	
`info`	Displays configured QoS characteristics for the eight QoS levels.
`egressmap 1p <level> <ieee1p>`	Maps the QoS level to IEEE 1p priority bits. Changes to this mapping table will not take effect until you save and reboot the switch. • `<level>` is the QoS level {0..7}. • `<ieee1p>` is the IEEE 802.1p bits {0..7}.
`egressmap ds <level> <dscp>`	Maps the QoS level to the DSCP. Changes to this mapping table will not take effect until you save and reboot the switch. • `<level>` is the QoS level {0..7}. • `<dscp>` is a 6-bit binary number.
`egressmap info`	Displays which DSCP and IEEE 802.1p levels are mapped to QoS levels for egress traffic.
`ingressmap 1p <ieee1p> <level>`	Maps the IEEE 802.1p bits to QoS levels. • `<ieee1p>` is the IEEE 802.1p priority level {0..7}. • `<level>` is the QoS level {0..7}.
`ingressmap ds <dscp> <level>`	Maps the DSCP to the QoS level. • `<dscp>` is a 6-bit binary number. • `<level>` is the QoS level {0..7}.
`ingressmap info`	Displays which DSCP and IEEE 802.1p levels are mapped to QoS levels for ingress traffic.
`queue <level> <weight>`	Configures the QoS queue. • `<level>` is the QoS Queue level index {0..7}. • `<weight>` is the QoS Queue weight {0..100}.

Figure 8-1 shows an example of the `config qos info` command.

```
Passport-8610:6# config qos info
                queue
                         level : 0
                        weight : 0
                queue
                         level : 1
                        weight : 6
                queue
                         level : 2
                        weight : 12
                queue
                         level : 3
                        weight : 18
                queue
                         level : 4
                        weight : 25
                queue
                         level : 5
                        weight : 31
                queue
                         level : 6
                        weight : 100
                queue
                         level : 7
                        weight : 6
```

Figure 8-1. *config qos info* Command Output

show qos queue Command

The `show qos queue` command shows the DiffServ queue settings for the eight queues on the switch. The queues are serviced using guaranteed Weighted Round Robin mechanism. QoS level 7 is reserved for network control traffic, and you cannot change the settings for that queue. Refer to the *Networking Concepts for the Passport 8000 Series Switch* for more information about these queues.

The command uses the syntax:

```
show qos queue
```

Figure 8-2 is an example.

```
Passport-8610# show qos queue

================================================================================
                                        Qos Queue Table
================================================================================
       SERVICE          ADMIN     OPER
LEVEL  CLASS            WEIGHT    WEIGHT
--------------------------------------------------------------------------------

0                       0         0

1      Standard         6         6

2      Bronze           12        12

3      Silver           18        18

4      Gold             25        25

5      Platinum         31        31

6      Premium          100       100

7      Net Control      6         6
```

Figure 8-2. *show qos queue* Command Output

IP Traffic Filters

IP filters on Passport switches can be used to manage traffic and, in some cases, to provide security. Each filter set includes match conditions and actions to be performed when a match condition is satisfied.

Packet filters apply to all routed packets to be forwarded through the switch on specified ingress ports. The filter sets are applied to the port and a default action (forward or drop) is set for the port. All packets not matching any filter take the default action; packets matching a single filter with the opposite action will take that action. For more explanation of filtering, refer to *Networking Concepts for the Passport 8000 Series Switch*.

config ip traffic-filter Commands

The following groups of commands are included:

- `config ip traffic-filter` commands
- `config ip traffic-filter create` commands
- `config ip traffic-filter filter` commands
- `config ip traffic-filter filter action` commands
- `config ip traffic-filter filter match` commands
- `config ip traffic-filter filter modify` commands
- `config ip traffic-filter global-set` commands
- `config ip traffic-filter set` commands
- config ip traffic-filter traffic-profile commands
- `config ethernet ip traffic-filter` commands

config ip traffic-filter Commands

The `config ip traffic-filter` commands have the following syntax and parameters:

config ip traffic-filter followed by:	
`info`	Displays which IP traffic filters are set for the `clear-stats` command.
`clear-stats [<fid>]`	Clears filter statistics for the specified filter ID. • `<fid>` is the traffic filter ID range of 1 to 4000.

config ip traffic-filter create Commands

The `config ip traffic-filter create` commands allow you to configure source, destination, and global traffic filters for the interface.

These commands use the following syntax and parameters:

config ip traffic-filter create followed by:	
`info`	Displays the destination, source, and global filters that have been created (Figure 8-3).
`destination dst-ip <value> [src-ip <value>]`	Creates a destination filter: • `dst-ip <value>` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `[src-ip <value>]` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
`global [src-ip <value>] [dst-ip <value>]`	Creates a global filter: • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x |default}. • `[dst-ip <value>]` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
`source src-ip <value> [dst-ip <value>]`	Creates a source filter: • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `[dst-ip <value>]` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
`traffic-profile <pid>`	Specifies a traffic profile to use with this traffic filter. • <pid> is the profile number {1..64}.

```
Passport-8610/config/ip/traffic-filter# create info

Sub-Context: create filter global-set set traffic-profile
Current Context:
                      global : (id 2)
                                 src-ip - 0.0.0.0/0.0.0.0
                                 dst-ip - 0.0.0.0/0.0.0.0
                      source : not created
                 destination : (id 1)
                               src-ip - 1.2.4.0/255.255.255.0
                               dst-ip - 1.2.3.0/255.255.255.0
             traffic-profile : (id 1)
```

Figure 8-3. *config ip traffic-filter create info* Command Output

config ip traffic-filter filter Commands

The `config ip traffic-filter filter` commands allow you to set up traffic filters where `<fid>` is the traffic filter ID (1 to 4000).

The commands take the following syntax and parameters:

config ip traffic-filter filter <fid> followed by:	
`info`	Displays the settings for the specified filter.
`delete`	Deletes the specified traffic filter.
`name <name>`	Names the filter. • `name <value>` is the IP filter name {string}.

config ip traffic-filter filter <fid> action Commands

The `config ip traffic-filter filter <fid> action` commands are used to set action parameters for IP filters by enabling or disabling the filters where `<fid>` is the traffic filter ID (1 to 4000).

The commands use the following syntax and parameters:

config ip traffic-filter filter <fid> action followed by:	
`info`	Displays configure actions for the filter.
`mode <default|forward|drop>`	Sets the action to occur when a filter is applied. • `<default|forward|drop>` are the choices: default action, forward the packet, or drop the packet.
`mirror <enable|disable>`	Enables or disables the traffic filter mirror option.
`statistic <enable|disable>`	Enables or disables the option to collect statistics on the traffic filter. The default setting is disable. If disabled, the `show ip traffic-filter stats` command will display zeros for this filter.

config ip traffic-filter filter <fid> action followed by:	
stop-on-match <true|false>	Stops further filtering if the current filter is applied.
tcp-connect <enable|disable>	Enables or disables the traffic filter TCP-connect option, which allows only TCP connections established from within the network (enabled) or allows bidirectional establishment (disabled). The default is disabled.

Figure 8-4 shows an example of the `config ip traffic-filter filter action info` command.

```
Passport-8610/config/ip/traffic-filter# filter 2 action info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                      mode : useDefaultAction
                    mirror : false
                statistics : disable
             stop-on-match : false
               tcp-connect : false
           traffic-profile : 0
```

Figure 8-4. *config ip traffic-filter filter action info* Command Output

config ip traffic-filter filter <fid> match Commands

The `config ip traffic-filter filter <fid> match` commands allow you to create matching criteria for filters. The commands require a `<fid>` that is the traffic filter ID (1 to 4000).

The commands use the following syntax and parameters:

config ip traffic-filter filter <fid> match followed by:	
info	Displays the matching settings for the filter.
ds-field <6-bit dscp> <2-bit reserved>	Sets the DS field to a specific number. This field is used to specify the match value for the DS field. The user must enter an 8-bit value, which is composed of the 6-bit DSCP and the 2-bit DSCP reserved fields. If the DS field in the incoming packet matches this value, then this filter will be applied to the packet. • <6-bit dscp> is a binary number. • <2-bit reserved> is a binary number.
ds-field-enable <enable|disable>	Enables or disables the traffic filter to match on the DS field set for the traffic filter.
dst-port <port> [dst-option <value>]	Sets the TCP/UDP destination port and destination option. • <port> is the TCP/UDP destination port to filter on (0 to 65535). • [dst-option <value>] is the TCP/UDP destination port option. {ignore|equal|less|greater|notequal}.
icmp-request <true|false>	Enables or disables the traffic filter to match ICMP requests.
ip-fragment <true|false>	Enables or disables the traffic filter to allow IP fragments to be filtered.
protocol <protocoltype>	Sets the protocol type for the filter. • <protocoltype> is {ignore|ICMP|TCP|UDP}.
src-port <port> [src-option <value>]	Sets the TCP/UDP source port and source option. • <port> is the TCP/UDP source port to filter on (0 to 65535). • [src-option <value>] is the option {ignore|equal|less|greater|notequal}.

Figure 8-5 shows an example of the `config ip traffic-filter filter match info` command.

```
Passport-8610:6/config/ip/traffic-filter/filter/1/match#
info

Sub-Context:
Current Context:

                    ds-field : 001000
           ds-field-reserved : 11
             ds-field-enable : disable
                icmp-request : false
                 ip-fragment : false
                    src-port : 0
                  src-option : ignore
                    dst-port : 0
                  dst-option : ignore
                    protocol : ignore
```

Figure 8-5. *config ip traffic-filter filter match info* Command Output

config ip traffic-filter filter <fid> modify Commands

The `config ip traffic-filter filter <fid> modify` commands allow you to modify traffic entering DiffServ access ports that meets the traffic filter. The commands require a traffic filter ID `<fid>` between 1 and 4000.

The commands use the following syntax and parameters:

config ip traffic-filter filter <fid> modify followed by:	
`info`	Displays the modify settings for the filter.
`dscp <6-bit dscp>`	If you want the DS codepoint (DSCP) modified to another value instead of zero, use this command to specify the value for the DSCP. After entering the binary number, you first must disable and then enable the traffic filter to ensure that it takes effect. • `<6-bit dscp>` is a binary number.
`dscp-enable <enable|disable>`	Enables or disables the traffic filter to modify the DSCP to zero on packets ingressing a DiffServ access port only.

config ip traffic-filter filter <fid> modify followed by:	
ieee8021p <integer>	If you want IEEE 802.1p bits modified to another value instead of zero, use this field to specify the value for the IEEE 802.1p bits. After entering the number, you first must disable and then enable the traffic filter to ensure that it takes effect. • <integer> is a number between 0 and 7.
ieee8021p-enable <enable|disable>	Enables or disables the traffic filter to modify the IEEE 802.1p bits to zero on packets ingressing a DiffServ access port only.

Note: When you enable a traffic filter to modify either the DSCP or IEEE 802.1p bits, the traffic filter will also modify the other value based on a corresponding value in the QoS ingress tables.

Figure 8-6 shows an example of `config ip traffic-filter filter modify info` command.

```
Passport-8610:6/config/ip/traffic-filter/filter/1/modify#
info

Sub-Context:
Current Context:

                          dscp : 000000
                   dscp-enable : disable
                     ieee8021p : 0
               ieee8021p-enable : disable
```

Figure 8-6. *config ip traffic-filter filter modify info* Command Output

config ip traffic-filter global-set Commands

The `config ip traffic-filter global-set` commands allow you to set a global filter and use a global set ID `<gsetid>` between 1 and 100.

The commands use the following syntax and parameters:

config ip traffic-filter global-set <gsetid> followed by:	
`info`	Displays the global set characteristics.
`add-filter <fid>`	Adds a global filter to a global set. • `<fid>` is the traffic filter ID range of 1 to 4000.
`create [name <value>]`	Creates a global set. • `[name <value>]` sets a name to the filter.
`delete`	Deletes a global set.
`remove-filter <fid>`	Removes a global filter from a global set. • `<fid>` is the traffic filter ID range of 1 to 4000.

Figure 8-7 shows an example of the `config ip traffic-filter global-set info` command.

```
Passport-8610/config/ip/traffic-filter# global-set 1 info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                    create :
                                name -
                    delete : N/A
                add-filter : 2
             remove-filter : N/A
```

Figure 8-7. *config ip traffic-filter global-set info* Command Output

config ip traffic-filter set Commands

The `config ip traffic-filter set` commands allow you to configure the source/destination set where `<setid>` is the set ID (300 to 1000). Only source/destination filters can be added to this set. You cannot add a global filter to it.

The commands use the following syntax and parameters:

config ip traffic-filter set <setid> followed by:	
info	Displays the filter set characteristics.
add-filter <fid>	Adds a filter to a filter set. • <fid> is the traffic filter ID range of 1 to 4000.
create [name <value>]	Creates a filter set. • name <value> is the set name {string}.
delete	Deletes a filter set.
remove-filter <fid>	Removes a filter from a filter set. • <fid> is the traffic filter ID range of 1 to 4000.

Figure 8-8 shows an example of the config ip traffic-filter set info command.

```
Passport-8610/config/ip/traffic-filter# set 301 info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                    create :
                                name -
                    delete : N/A
                add-filter :
             remove-filter : N/A
```

Figure 8-8. *config ip traffic-filter set info* Command Output

config ip traffic-filter traffic-profile <pid> Commands

The config ip traffic-filter traffic-profile <pid> commands allow you to set rate limiting profiles to police traffic streams. These commands use a Profile ID <pid> between 1 and 64.

The commands take the following syntax and parameters:

config ip traffic-filter traffic-profile <pid> followed by:	
info	Displays the traffic profile settings.
average-rate <int>	Sets the traffic profile's average rate. See "Implementation of Rate Limiting in the Passport 8000 Series Switch" for more information. • <int> is the rate {0..65535}, which is expressed in 64-byte segments of data allowed in a 2.5 millisecond timeslot.
delete	Deletes the traffic profile.
discard-out-profile <enable|disable>	Enables or disables the ability to discard the traffic that violates the traffic profile's average rate.
enable <true|false>	Enables or disables the traffic profile.
in-dscp <value>	Marks traffic that conforms to the average rate in the traffic profile. • <value> is the DSCP expressed as a 6-bit binary number.
name <name>	Names the traffic profile. • <name> is a string of 0 to 32 characters.
out-dscp <value>	Marks traffic that falls outside the traffic profile's average rate. • <value> is the DSCP expressed as a 6-bit binary number.
translate-dscp <enable|disable>	Enables or disables remarking of traffic as either in-dscp or out-dscp. This command must be enabled for any traffic to be marked.

Implementation of Rate Limiting in the Passport 8000 Series Switch

In the Passport 8000 Series switch, QoS rate metering is accomplished in increments of 64 bytes every 2.5 milliseconds. Tables 8-1, 8-2, and 8-3 present the measured line rates, in multiples of 64, for the three Ethernet speeds tested, with the expected results. The rates were obtained using a source/destination filter. Refer to *Networking Concepts for the Passport 8000 Series Switch* for more information about rate metering.

The three tables illustrate the effective throughput in megabits per second (Mb/s) for various traffic flows using different rate limiting values. All traffic loads are at 100% of interface speed, using fixed-sized packets of the size indicated (in bytes). Using these tables, you can determine the appropriate Average Rate Value that will give you the metering rate you desire.

The Target Average Rate for each interface type is shown, in increments of 10% of total interface speed, to help you determine the appropriate average-rate value to use for that interface. The actual throughput rate typically differs slightly from the target rate as illustrated.

For example, to configure a traffic profile with an average rate limit of 50% of a 100 Mb/s interface (or 50 Mb/s), enter 250 in the `average-rate` field in the CLI. Traffic is then limited to 51.23 Mb/s to 53.47 Mb/s, depending on the size of the packets.

Table 8-1. 10 Mb Ethernet Line Rate Metering

	average-rate <int>									
	5	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**	**50**
Packet size in bytes	**10%***	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
64	1.03†	2.05	3.08	4.10	5.12	6.15	7.17	7.62	7.62	7.62
128	1.23	2.05	3.28	4.10	5.33	6.15	7.38	8.20	8.65	8.65
256	1.64	2.46	3.28	4.10	5.74	6.56	7.38	8.19	9.28	9.28
512	1.64	3.28	3.28	4.92	6.56	6.56	8.20	8.20	9.62	9.62
1024	3.28	3.28	3.28	6.56	6.56	6.56	9.81	9.81	9.81	9.81
1518	4.86	4.86	4.86	4.86	9.72	9.72	9.72	9.72	9.72	9.87

* target average percentage of line rate

† rate in megabits per second

Table 8-2. 100 Mb Ethernet Line Rate Metering

	average-rate <int>									
	50	**100**	**150**	**200**	**250**	**300**	**350**	**400**	**450**	**500**
Packet size in bytes	**10%**	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
64	10.25	20.49	30.74	40.99	51.23	61.15	71.72	76.19	76.19	76.19
128	10.25	20.49	30.74	40.99	51.24	61.48	71.72	81.97	86.49	86.49
256	10.66	20.47	31.11	40.93	51.58	61.40	72.04	81.97	92.62	92.75
512	11.48	21.32	31.15	40.99	52.46	62.29	72.13	81.97	93.44	96.24
1024	13.12	22.96	32.80	42.63	52.46	62.30	72.13	81.97	95.08	98.08
1518	14.58	24.31	34.02	43.75	53.47	68.05	77.77	87.49	97.20	98.70

Table 8-3. Gigabit Ethernet Line Rate Metering

	average-rate <int>									
	500	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**	**5000**
Packet size in bytes	**10%**	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
64	102.50	205.00	307.47	409.93	446.61	446.61	446.61	446.61	446.61	446.61
128	102.50	204.93	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
256	102.49	204.96	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
512	103.32	204.99	308.30	409.86	513.13	614.79	718.07	819.68	922.93	962.41
1024	104.92	206.57	308.23	409.96	514.85	616.45	718.07	819.68	924.57	980.84
1518	106.93	213.89	320.90	422.93	529.87	636.78	743.68	845.72	952.62	986.99

Figure 8-9 shows an example of the `config ip traffic-filter traffic-profile info`

```
Passport-8610:5# config ip traffic-filter traffic-profile 1 info

Sub-Context: clear config dump monitor show test trace
Current Context:

                        name : test
                      enable : true
               translate-dscp : disable
                      in-dscp : 000000
                     out-dscp : 000000
           discard-out-profile : enable
                  average-rate : 0
```

Figure 8-9. *config ip traffic-filter traffic-profile info* Command Output

config ethernet <ports> ip traffic-filter Commands

The `config ethernet <ports> ip traffic-filter` commands allow you to set filters at the port level to manage traffic. Each filter set includes match conditions and actions to be performed when a match condition is satisfied. These commands include `<ports>` as the port list {slot/port[-slot/port][,...]}.

`config ethernet <ports> ip traffic-filter` `followed by:`	
`info`	Displays the traffic filters applied to the port.
`add set <value>`	Adds a set filter to a port. • `set <value>` is the global or source/destination filter set ID (1 to 1000).
`create`	Creates a traffic filtering entity on a port.
`default-action forward`	Sets the port filter default action to forward.
`default-action drop`	Sets the port filter default action to drop.
`default-action info`	Displays the port default action configuration.
`default-action none`	Does not apply any policy to filtered ports.
`delete`	Removes filtering from a port.

config ethernet <ports> ip traffic-filter followed by:	
disable	Disables filtering on a port. **Note:** Whenever you change a filter parameter, you must first disable the filter on its filter ports and then enable the filter again to reapply the changed filter to the ports.
enable	Enables filtering on a port. **Note:** Whenever you change a filter parameter, you must first disable the filter on its filter ports and then enable the filter again to reapply the changed filter to the ports.
remove set <value>	Removes a filter set from a port. • set <value> is the filter set ID (1 to 1000).

For more detailed information about the specific forward/drop behavior of a port, refer to *Networking Concepts for the Passport 8000 Series Switch*.

show ip traffic-filter Commands

The following commands provide information about the IP traffic filters.

show ip traffic-filter active Command

The `show ip traffic-filter active` command displays the list of active filters or returns the information that there are no active filters.

show ip traffic-filter destination Command

The `show ip traffic-filter destination` command displays the source and destination(s) for the active destination traffic filter(s). If a filter ID `<fid>` is entered, data is displayed for the specific filter; otherwise, all filters are shown.

The command uses the syntax:

```
show ip traffic-filter destination [<fid>]
```

Figure 8-10 shows the display for one filter ID.

```
Passport-8610# show ip traffic-filter destination

================================================================================
Ip Traffic-filter Destination Filters
================================================================================

ID  NAME           TYPE           SRC_OPTION DST_OPTION PROTOCOL   MIRROR
1                  destination     ignore     ignore     ignore     false

DST_ADDR        DST_MASK        DSTPT SRC_ADDR        SRC_MASK        SRCPT
    0.0.0.0         0.0.0.0         0     0.0.0.0         0.0.0.0         0

    TCPCONNECT      MODE            STOP_ON_MATCH
    false           useDefaultAction true

    DS_MT_DS_FIELD  DS_MT_DS_RSVED  DS_MD_8021P     DS_MD_DSCP
    000000          00:disable      0:enable        100011:enable

    DS_PRO_ID       M_ICMP_REQ      M_IP_FRAG       STATISTICS
    0               false           false           disable
```

Figure 8-10. *show ip traffic-filter destination* Command Output

show ip traffic-filter disabled Command

The `show ip traffic-filter disabled` command displays information about the disabled filters on the switch. If port numbers are entered, information is displayed only for those ports.

This command uses the format:

```
show ip traffic-filter disabled [<ports>]
```

show ip traffic-filter enabled Command

The `show ip traffic-filter enabled` command displays information about the enabled filters on the switch or on specified port.

This command uses the syntax:

```
show ip traffic-filter enabled [<ports>]
```

show ip traffic-filter global Command

The `show ip traffic-filter global` command displays global filters for the switch or for the specified filter IDs.

This command uses the syntax:

```
show ip traffic-filter global [<fid>].
```

Figure 8-11 is a display showing all filters.

```
Passport-8610:5/show/ip/traffic-filter# global

================================================================================
                                        Ip Traffic-filter Global Filters
================================================================================

ID  NAME           TYPE           SRC_OPTION DST_OPTION PROTOCOL   MIRROR
1   global-1        global          ignore     ignore     ignore     false

    DST_ADDR        DST_MASK        DSTPT SRC_ADDR        SRC_MASK
SRCPT
    0.0.0.0         0.0.0.0         0     0.0.0.0         0.0.0.0         0

    TCPCONNECT      MODE             STOP_ON_MATCH
    false           useDefaultAction true

    DS_MT_DS_FIELD  DS_MT_DS_RSVED  DS_MD_8021P     DS_MD_DSCP
    000000          00:disable      0:enable        100011:enable

    DS_PRO_ID       M_ICMP_REQ      M_IP_FRAG       STATISTICS
    0               false           false           disable
```

Figure 8-11. *show ip traffic-filter global* Command Output

show ip traffic-filter info global-set Command

The `show ip traffic-filter info global-set` command displays information about the specified global filter list or all global filter lists on the switch.

This command uses the syntax:

```
show ip traffic-filter info global-set [<id>]
```

Figure 8-12 is a display for list ID 1.

```
Passport-8606# show ip traffic-filter info global-set 1

================================================================================
                                        Ip Traffic-filter Global List
================================================================================

ID    NAME                 LIST_SIZE  FILTER_ID_LIST
--------------------------------------------------------------------------------
1                          1          2
```

Figure 8-12. *show ip traffic-filter info global-set* Command Output

show ip traffic-filter info set Command

The `show ip traffic-filter info set` command displays information for the specified source/destination filter list or all source/destination filter lists.

This command uses the syntax:

```
show ip traffic-filter info set [<id>]
```

Figure 8-13 is a display of the command.

```
Passport-8606# show ip traffic-filter info set

=========================================================================
Ip Traffic-filter Base List
=========================================================================

ID    NAME                 LIST_SIZE  FILTER_ID_LIST
-------------------------------------------------------------------------
301                        0
```

Figure 8-13. *show ip traffic-filter info set* Command Output

show ip traffic-filter interface Command

The `show ip traffic-filter interface` command displays information about the traffic filter interface for the switch or for specified ports.

This command uses the syntax:

```
show ip traffic-filter interface <ports>
```

Figure 8-14 is a sample display for port 9/2.

```
Passport-8606# show ip traffic-filter interface 9/2

=============================================================
Ip Traffic-filter Interface
=============================================================

                        IfIndex : 577
                 FilterListSize : 1
                     FilterList : 301
                         Enable : false
                  DefaultAction : none
```

Figure 8-14. *show ip traffic-filter interface* Command Output

show ip traffic-filter source Command

The `show ip traffic-filter source` command displays information about the active source traffic filter.

This command uses the syntax:

```
show ip traffic-filter source [<fid>]
```

show ip traffic-filter stats Command

The `show ip traffic-filter stats` command displays the filter ID and counter information for all filters or the specified filter ID that have statistics gathering enabled.

This command uses the syntax:

```
show ip traffic-filter stats [<fid>]
```

Figure 8-15 is a sample.

```
Passport-8610# show ip traffic-filter stats

================================================================================
                                      Ip Traffic-filter Stats
================================================================================
        FILTER ID       DISCARD PKTS    FILTER-OCTETS   FILTER-PKTs
--------------------------------------------------------------------------------
           1            0               0               0
           2            0               0               0
```

Figure 8-15. *show ip traffic-filter stats* Command Output

show ip traffic-filter traffic-profile info Command

The `show ip traffic-filter traffic-profile info` command displays the traffic profile settings.

This command uses the syntax:

```
show ip traffic-filter traffic-profile info [<id>]
```

Figure 8-16 is a sample.

```
Passport-8610:5/show/ip/traffic-filter/traffic-profile# info

================================================================================
                                        Ip Traffic-filter Profile
================================================================================

ID  NAME       ENABLE     TRANS_DSFIELD   IN_DSFIELD      OUT_DSFIELD
1              true       enable          11111111 11111111

    DISCARD_OUT_PROFILE   AVERAGE_RATE
    enable                0
```

Figure 8-16. *show ip traffic-filter traffic-profile* Command Output

Appendix A
CLI Command List

This appendix provides the complete CLI command list in alphabetical order, with the approximate page reference for the beginning pages of further explanations. Boldface type in Table A-1 indicates commands that are new in this release or have add functionality. Commands that were in the previous release or that have changed in syntax or in position in the command tree but add no new functionality are listed in normal type.

Table A-1. CLI Command List

config ethernet <ports> ip arp-response disable config ethernet <ports> ip arp-response enable config ethernet <ports> ip arp-response info	page 1-13
config ethernet <ports> ip create <ipaddr/mask> <vid> [mac_offset <value>] config ethernet <ports> ip delete <ipaddr>	page 1-6
config ethernet <ports> ip dhcp-relay broadcast <enable|disable> config ethernet <ports> ip dhcp-relay disable config ethernet <ports> ip dhcp-relay enable config ethernet <ports> ip dhcp-relay info config ethernet <ports> ip dhcp-relay max-hop <max-hop> config ethernet <ports> ip dhcp-relay min-sec <min-sec> config ethernet <ports> ip dhcp-relay mode <mode>	page 2-4
config ethernet <ports> ip dvmrp enable config ethernet <ports> ip dvmrp disable config ethernet <ports> ip dvmrp info config ethernet <ports> ip dvmrp metric <cost>	page 5-9
config ethernet <ports> ip l3-igmp info config ethernet <ports> ip l3-igmp last-memb-query-int <seconds> config ethernet <ports> ip l3-igmp query-interval <seconds> config ethernet <ports> ip l3-igmp query-max-resp <seconds> config ethernet <ports> ip l3-igmp robustval <integer> config ethernet <ports> ip l3-igmp version <integer>	page 5-16

Table A-1. CLI Command List (continued)

config ethernet <ports> ip ospf advertise-when-down <enable|disable>	page 3-27
config ethernet <ports> ip ospf area <ipaddr>	
config ethernet <ports> ip ospf authentication-key <string>	
config ethernet <ports> ip ospf authentication-type <auth-type>	
config ethernet <ports> ip ospf disable	
config ethernet <ports> ip ospf enable	
config ethernet <ports> ip ospf hello-interval <seconds>	
config ethernet <ports> ip ospf dead-interval <seconds>	
config ethernet <ports> ip ospf info	
config ethernet <ports> ip ospf metric <cost>	
config ethernet <ports> ip ospf priority <integer>	
config ethernet <ports> ip proxy disable	page 1-13
config ethernet <ports> ip proxy enable	
config ethernet <ports> ip proxy info	
config ethernet <ports> ip rip advertise-when-down <enable|disable>	page 3-4
config ethernet <ports> ip rip auto-aggr <enable|disable>	
config ethernet <ports> ip rip default-listen <enable|disable>	
config ethernet <ports> ip rip default-supply <enable|disable>	
config ethernet <ports> ip rip disable	
config ethernet <ports> ip rip enable	
config ethernet <ports> ip rip info	
config ethernet <ports> ip rip listen <enable|disable>	
config ethernet <ports> ip rip manualtrigger	
config ethernet <ports> ip rip poison <enable|disable>	
config ethernet <ports> ip rip supply <enable|disable>	
config ethernet <ports> ip rip trigger <enable|disable>	
config ethernet <ports> ip traffic-filter add set <value>	page 8-18
config ethernet <ports> ip traffic-filter create	
config ethernet <ports> ip traffic-filter default-action forward	
config ethernet <ports> ip traffic-filter default-action drop	
config ethernet <ports> ip traffic-filter default-action info	
config ethernet <ports> ip traffic-filter default-action none	
config ethernet <ports> ip traffic-filter delete	
config ethernet <ports> ip traffic-filter disable	
config ethernet <ports> ip traffic-filter enable	
config ethernet <ports> ip traffic-filter info	
config ethernet <ports> ip traffic-filter remove set <value>	

Table A-1. CLI Command List (continued)

config ethernet <ports> ip vrrp <vrid> address <ipaddr> config ethernet <ports> ip vrrp <vrid> adver-int <seconds> config ethernet <ports> ip vrrp <vrid> critical-ip <ipaddr> config ethernet <ports> ip vrrp <vrid> delete config ethernet <ports> ip vrrp <vrid> disable config ethernet <ports> ip vrrp <vrid> enable config ethernet <ports> ip vrrp <vrid> info config ethernet <ports> ip vrrp <vrid> priority <prio>	page 4-1
config ip arp add ports <value> ip <value> mac <value> [vlan <value>] config ip arp aging <minutes> config ip arp delete <ipaddr> config ip arp info	page 1-11
config ip default-ttl <seconds>	page 1-1
config ip dhcp-relay create-fwd-path agent <value> server <value> [mode <value>] [state <value>] config ip dhcp-relay enable-fwd-path agent <value> server <value> config ip dhcp-relay delete-fwd-path agent <value> server <value> config ip dhcp-relay disable-fwd-path agent <value> server <value> config ip dhcp-relay info config ip dhcp-relay mode <mode> agent <value> server <value>	page 2-2
config ip dvmrp disable config ip dvmrp enable config ip dvmrp info config ip dvmrp interface <ipaddr> disable config ip dvmrp interface <ipaddr> enable config ip dvmrp interface <ipaddr> info config ip dvmrp interface <ipaddr> metric <cost> config ip dvmrp leaf-timeout <integer> config ip dvmrp nbr-timeout <integer> config ip dvmrp nbr-probe-interval <integer> config ip dvmrp triggered-update-interval <integer> config ip dvmrp update-interval <integer>	page 5-4
config ip forwarding disable config ip forwarding enable config ip forwarding info	page 1-1
config ip l3-igmp info config ip l3-igmp interface <ipaddr> info config ip l3-igmp interface <ipaddr> last-memb-query-int <seconds> config ip l3-igmp interface <ipaddr> query-interval <seconds> config ip l3-igmp interface <ipaddr> query-max-resp <integer> config ip l3-igmp interface <ipaddr> robustval <integer> config ip l3-igmp interface <ipaddr> version <integer> **config ip l3-igmp interface <ipaddr> admin-version <integer>**	page 5-13

Table A-1. CLI Command List (continued)

config ip mroute info config ip mroute interface <ipaddr> info config ip mroute interface <ipaddr> ttl <ttl>	page 5-1
config ip ospf admin-state <enable|disable>	page 3-10
config ip ospf area <ipaddr> create config ip ospf area <ipaddr> delete config ip ospf area <ipaddr> import-summaries <true|false> config ip ospf area <ipaddr> info config ip ospf area <ipaddr> nssa <true|false> config ip ospf area <ipaddr> range <ipaddr/mask> create advertise-mode <value> lsa-type <value> config ip ospf area <ipaddr> range <ipaddr/mask> delete config ip ospf area <ipaddr> range <ipaddr/mask> info config ip ospf area <ipaddr> stub <true|false> config ip ospf area <ipaddr> stub-metric <stub-metric> config ip ospf area <ipaddr> virtual-interface <nbr> add-message-digest-key <md5-key-id> md5-key <value> config ip ospf area <ipaddr> virtual-interface <nbr> authentication-key <authentication-key> config ip ospf area <ipaddr> virtual-interface <nbr> authentication-type <auth-type> config ip ospf area <ipaddr> virtual-interface <nbr> create config ip ospf area <ipaddr> virtual-interface <nbr> delete config ip ospf area <ipaddr> virtual-interface <nbr> delete-message-digest-key <md5-key-id> config ip ospf area <ipaddr> virtual-interface <nbr> hello-interval <seconds> config ip ospf area <ipaddr> virtual-interface <nbr> dead-interval <seconds> config ip ospf area <ipaddr> virtual-interface <nbr> info config ip ospf area <ipaddr> virtual-interface <nbr> retransmit-interval <seconds> config ip ospf area <ipaddr> virtual-interface <nbr> transit-delay <seconds>	page 3-15
config ip ospf as-boundary-router <enable|disable> config ip ospf auto-vlink <enable|disable> config ip ospf default-metric [ethernet <value>] [fast-ethernet <value>] [gig-ethernet <value>] config ip ospf disable config ip ospf enable config ip ospf holddown <seconds>	page 3-11
config ip ospf host-route <ipaddr> create config ip ospf host-route <ipaddr> delete config ip ospf host-route <ipaddr> info config ip ospf host-route <ipaddr> metric <metric>	page 3-12

Table A-1. CLI Command List (continued)

config ip ospf info	page 3-11
config ip ospf interface <ipaddr> add-message-digest-key <md5-key-id> md5-key <value>	page 3-13
config ip ospf interface <ipaddr> admin-status <enable|disable>	
config ip ospf interface <ipaddr> area <ipaddr>	
config ip ospf interface <ipaddr> authentication-key <authentication-key>	page 3-13
config ip ospf interface <ipaddr> authentication-type <auth-type>	
config ip ospf interface <ipaddr> delete-message-digest-key <md5-key-id>	
config ip ospf interface <ipaddr> hello-interval <seconds>	
config ip ospf interface <ipaddr> dead-interval <seconds>	
config ip ospf interface <ipaddr> info	
config ip ospf interface <ipaddr> metric <metric>	
config ip ospf interface <ipaddr> poll-interval <seconds>	
config ip ospf interface <ipaddr> priority <priority>	
config ip ospf interface <ipaddr> retransmit-interval <seconds>	
config ip ospf interface <ipaddr> transit-delay <seconds>	
config ip ospf router-id <ipaddr>	
config ip ospf trap <enable|disable>	
config ip policy addrlist <listid> add-address <ipaddr>	page 7-2
config ip policy addrlist <listid> create	
config ip policy addrlist <listid> delete	
config ip policy addrlist <listid> info	
config ip policy addrlist <listid> name <name>	
config ip policy addrlist <listid> remove-address <ipaddr>	
config ip policy netlist <listid> add-network <ipaddr/mask>	page 7-3
config ip policy netlist <listid> create	
config ip policy netlist <listid> delete	
config ip policy netlist <listid> info	
config ip policy netlist <listid> name <name>	
config ip policy netlist <listid> remove-network <ipaddr/mask>	
config ip policy ospf accept <pid> action <accept|ignore>	page 7-4
config ip policy ospf accept <pid> create	
config ip policy ospf accept <pid> delete	
config ip policy ospf accept <pid> disable	
config ip policy ospf accept <pid> enable	
config ip policy ospf accept <pid> exact-net-list <netlist id>	
config ip policy ospf accept <pid> ext-metric-type <type1|type2>	
config ip policy ospf accept <pid> info	
config ip policy ospf accept <pid> inject-net-list <netlist id>	
config ip policy ospf accept <pid> name <string>	
config ip policy ospf accept <pid> precedence <precedence>	
config ip policy ospf accept <pid> range-net-list <netlist id>	

Table A-1. CLI Command List (continued)

config ip policy ospf announce <pid> action <announce|ignore>	page 7-6
config ip policy ospf announce <pid> add-route-source <direct|static|rip|any>	
config ip policy ospf announce <pid> advertise-netlist <netlist id>	
config ip policy ospf announce <pid> create	
config ip policy ospf announce <pid> delete	
config ip policy ospf announce <pid> disable	
config ip policy ospf announce <pid> enable	
config ip policy ospf announce <pid> exact-netlist <netlist id>	
config ip policy ospf announce <pid> ext-metric <ext-metric>	
config ip policy ospf announce <pid> ext-metric-type <type1|type2>	
config ip policy ospf announce <pid> info	
config ip policy ospf announce <pid> name <string>	
config ip policy ospf announce <pid> precedence <precedence>	
config ip policy ospf announce <pid> range-netlist <netlist id>	
config ip policy ospf announce <pid> remove-route-source <direct|static|rip|any>	
config ip policy ospf announce <pid> rip-gateway-list <addrlist id>	
config ip policy ospf announce <pid> rip-interface-list <addrlist id>	
config ip policy ospf apply-accept	page 7-4
config ip policy ospf apply-announce	
config ip policy ospf info	
config ip policy rip accept <pid> action <accept|ignore>	page 7-8
config ip policy rip accept <pid> apply-mask <ipmask>	
config ip policy rip accept <pid> create	
config ip policy rip accept <pid> delete	
config ip policy rip accept <pid> disable	
config ip policy rip accept <pid> enable	
config ip policy rip accept <pid> exact-netlist <netlist id>	
config ip policy rip accept <pid> info	
config ip policy rip accept <pid> inject-netlist <netlist id>	
config ip policy rip accept <pid> name <string>	
config ip policy rip accept <pid> precedence <precedence>	
config ip policy rip accept <pid> range-netlist <netlist id>	
config ip policy rip accept <pid> rip-gateway-list <addrlist id>	
config ip policy rip accept <pid> rip-interface-list <listid>	

Table A-1. CLI Command List (continued)

config ip policy rip announce <pid> action <announce|ignore> config ip policy rip announce <pid> add-route-source <direct|static|rip|ospf|any> config ip policy rip announce <pid> advertise-netlist <netlist id> config ip policy rip announce <pid> create config ip policy rip announce <pid> delete config ip policy rip announce <pid> disable config ip policy rip announce <pid> enable config ip policy rip announce <pid> exact-netlist <netlist id> config ip policy rip announce <pid> info config ip policy rip announce <pid> name <string> config ip policy rip announce <pid> ospf-router-id-list <addrlist id> config ip policy rip announce <pid> ospf-route-type <type1|type2|external|internal|any> config ip policy rip announce <pid> outbound-interface-list <addrlist id> config ip policy rip announce <pid> precedence <precedence> config ip policy rip announce <pid> range-netlist <netlist id> config ip policy rip announce <pid> remove-route-source <direct|static|rip|ospf|any> config ip policy rip announce <pid> rip-gateway-list <addrlist id> config ip policy rip announce <pid> rip-interface-list <addrlist id> config ip policy rip announce <pid> rip-metric <rip-metric> config ip policy rip info	page 7-10
config ip rip disable config ip rip domain <ipaddr> <value> config ip rip enable config ip rip holddown <seconds> config ip rip info config ip rip updatetime <seconds> config ip rip receive <ipaddr> mode <value> config ip rip send <ipaddr> mode <value>	page 3-1
config ip route delete <ipaddr/mask> **config ip route info** config ip route-discovery disable config ip route-discovery enable config ip route-discovery info	page 1-1
config ip static-route create <ipaddr/mask> next-hop <value> cost <value> config ip static-route delete <ipaddr/mask> next-hop <value> **config ip static-route disable <ipaddr/mask> next-hop <value>** **config ip static-route enable <ipaddr/mask> next-hop <value>** config ip static-route info	page 1-1
config ip traffic-filter clear-stats [<fid>] config ip traffic-filter create destination dst-ip <value> [src-ip <value>] config ip traffic-filter create global [src-ip <value>] [dst-ip <value>] config ip traffic-filter create info config ip traffic-filter create traffic-profile <pid> config ip traffic-filter create source src-ip <value> [dst-ip <value>]	page 8-6

Table A-1. CLI Command List (continued)

config ip traffic-filter filter <fid> action mode <default|forward|drop> config ip traffic-filter filter <fid> action info config ip traffic-filter filter <fid> action mirror <enable|disable> **config ip traffic-filter filter <fid> action statistic <enable|disable>** **config ip traffic-filter filter <fid> action stop-on-match <true|false>** config ip traffic-filter filter <fid> action tcp-connect <enable|disable> **config ip traffic-filter filter <fid> action traffic-profile <integer>**	page 8-8
config ip traffic-filter filter <fid> delete config ip traffic-filter filter <fid> info	page 8-8
config ip traffic-filter filter <fid> match ds-field <integer> **config ip traffic-filter filter <fid> match ds-field-enable <enable|disable>** config ip traffic-filter <fid> match dst-port <port> [dst-option <value>] **config ip traffic-filter <fid> match igmp-request <true|false>** **config ip traffic-filter <fid> match ieee8021p <integer>** **config ip traffic-filter <fid> match ieee8021p-enable <enable|disable>** config ip traffic-filter <fid> match info **config ip traffic-filter <fid> match ip-fragment <true|false>** config ip traffic-filter <fid> match protocol <prototypal> config ip traffic-filter <fid> match src-port <port> [src-option <value>]	page 8-9
config ip traffic-filter <fid> modify ds-field <integer> **config ip traffic-filter <fid> modify ds-field-enable <enable|disable>** **config ip traffic-filter <fid> modify ieee8021p <integer>** **config ip traffic-filter <fid> modify ieee8021p-enable <enable|disable>** config ip traffic-filter <fid> modify info	page 8-11
config ip traffic-filter <fid> name <name>	page 8-6
config ip traffic-filter global-set <gusted> add-filter <fid> config ip traffic-filter global-set <gusted> create [name <value>] config ip traffic-filter global-set <gusted> delete config ip traffic-filter global-set <gusted> info config ip traffic-filter global-set <gusted> remove-filter <fid>	page 8-13
config ip traffic-filter info	page 8-6
config ip traffic-filter set <sited> add-filter <fid> config ip traffic-filter set <sited> create [name <value>] config ip traffic-filter set <sited> delete config ip traffic-filter set <sited> info config ip traffic-filter set <sited> remove-filter <fid>	page 8-13

Table A-1. CLI Command List (continued)

config ip traffic-filter traffic-profile <pid> average-rate <in> **config ip traffic-filter traffic-profile <pid> delete** **config ip traffic-filter traffic-profile <pid> discard-out-profile <enable|disable>** **config ip traffic-filter traffic-profile <pid> enable <true|false>** **config ip traffic-filter traffic-profile <pid> in-dissolved <in>** **config ip traffic-filter traffic-profile <pid> info** **config ip traffic-filter traffic-profile <pid> name <name>** **config ip traffic-filter traffic-profile <pid> out-dissolved <in>** **config ip traffic-filter traffic-profile <pid> translate-ds-field <enable|disable>**	page 8-14
config ip udpfwd info	page 2-8
config ip udpfwd interface <ipaddr> create <fwdlistid> config ip udpfwd interface <ipaddr> delete config ip udpfwd interface <ipaddr> info config ip udpfwd interface <ipaddr> maxttl <maxttl> config ip udpfwd interface <ipaddr> udpportfwdlist <fwdlistid>	page 2-9
config ip udpfwd portfwdlist <fwdlistid> add-portfwd <udpport> <ipaddr> config ip udpfwd portfwdlist <fwdlistid> create config ip udpfwd portfwdlist <fwdlistid> delete config ip udpfwd portfwdlist <fwdlistid> info config ip udpfwd portfwdlist <fwdlistid> name <name> config ip udpfwd portfwdlist <fwdlistid> remove-portfwd <udpport> <ipaddr>	page 2-9
config ip udpfwd protocol <udpport> create <protoname> config ip udpfwd protocol <udpport> delete config ip udpfwd protocol <udpport> info	page 2-8
config ipx forwarding disable [<IPX-network-number>] config ipx forwarding enable [<IPX-network-number>] config ipx forwarding info	page 6-3
config ipx info	page 6-3
config ipx rip default-delay <delay-timer> config ipx rip default-hold-multiplier <hold-multiplier> config ipx rip default-interval <interval-timer> config ipx rip hold-multiplier <IPX-network-number> <hold-multiplier> config ipx rip info config ipx rip update-delay <IPX-network-number> <delay-timer> config ipx rip update-interval <IPX-network-number> <interval-timer>	page 6-7

Table A-1. CLI Command List (continued)

config ipx sap create <service-type> <service-name> <ipxhost> <socket-number> <hop-count> config ipx sap delete <service-name> config ipx sap default-delay <delay-timer> config ipx sap default-hold-multiplier <hold-multiplier> config ipx sap default-interval <interval-timer> config ipx sap hold-multiplier <IPX-network-number> <hold-multiplier> config ipx sap info config ipx sap update-delay <IPX-network-number> <delay-timer> config ipx sap update-interval <IPX-network-number> <interval-timer>	page 6-8
config ipx set max-route <max_entries> config ipx set max-sap <max_entries> config ipx set max-static-route <max_entries> config ipx set max-static-sap <max_entries> config ipx set info **config ipx set netbios <on|off>**	page 6-4
config ipx static-route create <IPX-network-number> <nexthop> <hop-count> <tick-count> config ipx static-route delete <IPX-network-number> config ipx static-route info	page 6-6
config vlan <vid> ip arp-response disable config vlan <vid> ip arp-response enable config vlan <vid> ip arp-response info	page 1-15
config vlan <vid> ip create <ipaddr/mask> [mac_offset <value>] config vlan <vid> ip delete <ipaddr>	page 1-9
config vlan <vid> ip dhcp-relay broadcast <enable|disable> config vlan <vid> ip dhcp-relay disable config vlan <vid> ip dhcp-relay enable config vlan <vid> ip dhcp-relay info config vlan <vid> ip dhcp-relay max-hop <max-hop> config vlan <vid> ip dhcp-relay min-sec <min-sec> config vlan <vid> ip dhcp-relay mode <mode>	page 2-6
config vlan <vid> ip dvmrp enable config vlan <vid> ip dvmrp disable config vlan <vid> ip dvmrp info config vlan <vid> ip dvmrp metric <cost>	page 5-11
config vlan <vid> ip l3-igmp info config vlan <vid> ip l3-igmp last-memb-query-int <seconds> config vlan <vid> ip l3-igmp query-interval <seconds> config vlan <vid> ip l3-igmp query-max-resp <seconds> config vlan <vid> ip l3-igmp robustval <integer> config vlan <vid> ip l3-igmp version <integer>	page 5-18

Table A-1. CLI Command List (continued)

config vlan <vid> ip info	page 1-9
config vlan <vid> ip ospf advertise-when-down <enable|disable> config vlan <vid> ip ospf area <ipaddr> config vlan <vid> ip ospf authentication-key <string> config vlan <vid> ip ospf authentication-type <auth-type> config vlan <vid> ip ospf disable config vlan <vid> ip ospf enable config vlan <vid> ip ospf hello-interval <seconds> config vlan <vid> ip ospf dead-interval <seconds> config vlan <vid> ip ospf info config vlan <vid> ip ospf metric <cost> config vlan <vid> ip ospf priority <integer>	page 3-31
config vlan <vid> ip proxy disable config vlan <vid> ip proxy enable config vlan <vid> ip proxy info	page 1-15
config vlan <vid> ip rip advertise-when-down <enable|disable> config vlan <vid> ip rip auto-aggr <enable|disable> config vlan <vid> ip rip default-listen <enable|disable> config vlan <vid> ip rip default-supply <enable|disable> config vlan <vid> ip rip disable config vlan <vid> ip rip enable config vlan <vid> ip rip info config vlan <vid> ip rip listen <enable|disable> config vlan <vid> ip rip manualtrigger config vlan <vid> ip rip poison <enable|disable> config vlan <vid> ip rip supply <enable|disable> config vlan <vid> ip rip trigger <enable|disable>	page 3-8
config vlan <vid> ip vrrp <vrid> address <ipaddr> config vlan <vid> ip vrrp <vrid> adver-int <seconds> config vlan <vid> ip vrrp <vrid> critical-ip <ipaddr> config vlan <vid> ip vrrp <vrid> delete config vlan <vid> ip vrrp <vrid> disable config vlan <vid> ip vrrp <vrid> enable config vlan <vid> ip vrrp <vrid> info config vlan <vid> ip vrrp <vrid> priority <prio>	page 4-4
config vlan <vid> ipx create <IPX-network-number> [<encapsulation>] config vlan <vid> ipx delete <IPX-network-number> config vlan <vid> ipx info	page 6-4

Table A-1. CLI Command List (continued)

config qos egressmap 1p <level> <ieee1p> **config qos egressmap ds <level> <ds-field>** **config qos egressmap info** **config qos info** **config qos ingressmap 1p <ieee1p> <level>** **config qos ingressmap ds <ds-field> <level>** **config qos ingressmap info** **config qos queue <level> <weight>**	page 8-3
show ip arp info [<ip address>] [-s <value>]	page 1-12
show ip dhcp-relay counters show ip dhcp-relay fwd-path	page 2-3
show ip dvmrp info show ip dvmrp interface show ip dvmrp neighbor show ip dvmrp next-hop show ip dvmrp route	page 5-6
show ip forwarding	page 1-4
show ip interface	page 1-4
show ip l3-igmp cache show ip l3-igmp group show ip l3-igmp interface	page 5-14
show ip mroute interface show ip mroute next-hop show ip mroute route	page 5-2
show ip ospf area show ip ospf ase [metric-type <value>] show ip ospf default-metric show ip ospf host-route show ip ospf ifstats [mismatch] [ifstats] show ip ospf info show ip ospf interface show ip ospf int-timers show ip ospf lsdb [area <value>] [lsatype <value>] [lsid <value>] [adv_rtr <value>] [detail] show ip ospf neighbors show ip ospf range show ip ospf stats	page 3-19

Table A-1. CLI Command List (continued)

show ip policy addrlist info [id <value>] show ip policy netlist info [id <value>] show ip policy ospf accept info [id <value>] show ip policy ospf accept lists [id <value>] show ip policy ospf accept match network <value> show ip policy ospf announce info [id <value>] show ip policy ospf announce lists [id <value>] show ip policy ospf announce match network <value>	page 7-12
show ip policy rip accept info [id <value>] show ip policy rip accept lists [id <value>] show ip policy rip accept match network <value> show ip policy rip announce info [id <value>] show ip policy rip announce lists [id <value>] show ip policy rip announce match network <value>	page 7-16
show ip route-discovery	page 1-4
show ip rip info show ip rip interface [<ipaddr>]	page 3-3
show ip route info [<ip address>] [-s <value>]	page 1-5
show ip static-route info [<ip address>] [-s <value>]	page 1-5
show ip traffic-filter active show ip traffic-filter destination [<fid>] show ip traffic-filter disabled [<ports>] show ip traffic-filter enabled [<ports>] show ip traffic-filter global [<fid>] show ip traffic-filter info global-set [<id>] show ip traffic-filter info set [<id>] show ip traffic-filter interface <ports> show ip traffic-filter source [<fid>] show ip traffic-filter stats [<fid>] **show ip traffic-filter traffic-profile info [<id>]**	page 8-19
show ip udpfwd interface info [<ipaddr>] show ip udpfwd portfwd info show ip udpfwd portfwdlist info [<fwdlistid>] show ip udpfwd protocol info	page 2-9
show ip vrrp info [<vrid>] [<ipaddr>] show ip vrrp stats <vrid> <ipaddr>	page 4-6
show ipx config [<IPX-network-number>] show ipx default show ipx route [<IPX-network-number>] [<IPX-network-number>] show ipx sap [<service-name>] show ipx stats <IPX-network-number>	page 6-11

Table A-1. CLI Command List (continued)

show qos egressmap 1p [<level>] **show qos egressmap ds [<level>]** **show qos ingressmap 1p [<ieee1p>]** **show qos ingressmap ds [<ds-field>]** **show qos queue [<level>]**	page 8-4
..	

Index

A

accept policy
  OSPF, 7-4
  RIP, 7-8

address list ID, 7-2

announce policy
  OSPF, 7-6
  RIP, 7-10

ARP commands
  configure, 1-10
  IP, 1-11
  port, 1-13
  show, 1-12
  VLAN, 1-15

C

CLI command list, A-1 to A-14

config ip policy commands, 7-1 to 7-12

customer support, xxvi

D

DHCP relay commands
  configure, 2-2
  port, 2-4
  show, 2-3
  VLAN, 2-6

Distance Vector Multicast Routing Protocol. *See* DVMRP

DVMRP commands
  configure, 5-4
  global, 5-4
  port, 5-9
  show, 5-6
  VLAN, 5-11

Dynamic Host Configuration Protocol. *See* DHCP

E

Ethernet port commands
  ARP configure, 1-13
  configure IP, 1-6
  OSPF configure, 3-27
  OSPF show, 3-29
  show IP info, 1-8
  VRRP, 4-1

I

IGMP commands
  IP, 5-13
  port, 5-16
  show, 5-14
  VLAN, 5-18

Internet Group Management Protocol. *See* IGMP

Internet Packet Exchange. *See* IPX

IP commands
  configure, 1-1
  show, 1-4

IP forwarding commands, 1-4

IP policies, 7-1

IP policy commands
  configure, 7-1 to 7-12
  show, 7-12 to 8-1

IP traffic filter commands
  configure, 8-6 to 8-14
  port, 8-18
  show, 8-19 to 8-24

IP traffic profile commands, 8-24
  configure, 8-14

IPX commands
configure, 6-2
RIP, 6-7
SAP, 6-8
set, 6-4
show, 6-11
static route, 6-6
VLAN, 6-4

L

link state database, 3-23

M

multicast commands, 5-1

N

network lists ID, 7-3

O

Open Shortest Path First. *See* OSPF
OSPF
accept policy, 7-4
announce policy, 7-6
OSPF commands
configure, 3-11 to 3-18
port, 3-27
show, 3-19
VLAN, 3-31

P

port ARP commands
configure, 1-13
show, 1-14
port commands
configure IP, 1-6
show IP info, 1-8
VRRP, 4-1
port DHCP commands
configure, 2-4
show, 2-5
port DVMRP commands
configure, 5-10
show, 5-10
port l3 IGMP commands, 5-16
port OSPF commands
configure, 3-27
show, 3-29
port RIP commands
configure, 3-4
show, 3-7
port traffic-filter commands, 8-18
port VRRP commands
configure, 4-1
show, 4-3
product support, xxvi
publications
Bay Networks related, xxiii
external related, xxv
hard copy, xxv

Q

QoS command
configure, 8-3 to 8-4
show, 8-4
Quality of Service. *See* QoS.

R

RFCs, xxv
RIP
accept policy, 7-8
announce policy, 7-10
RIP commands
IP, 3-1
port, 3-4
show, 3-3
VLAN, 3-8
Routing Information Protocol. *See* RIP

S

show, 8-24
show ports stats routing commands, 5-3
support, Nortel Networks, xxvi

T

technical publications, xxv

technical support, xxvi

traffic filters. *See* IP traffic filter commands

U

UDP commands
  configure, 2-8
  show, 2-10

User Data Protocol. *See* UDP commands

V

Virtual Router Redundancy Protocol. *See* VRRP commands

VLAN ARP commands
  configure, 1-15
  show, 1-16

VLAN DHCP commands
  configure, 2-6
  show, 2-7

VLAN DVMRP commands
  configure, 5-11
  show, 5-12

VLAN IP commands, 1-9

VLAN IPX commands, 6-4

VLAN l3 IGMP commands, 5-18

VLAN OSPF commands
  configure, 3-31
  show, 3-33

VLAN RIP commands
  configure, 3-8
  show, 3-10

VLAN VRRP commands
  configure, 4-4
  show, 4-5

VRRP commands
  port, 4-1
  show, 4-6, 4-7
  VLAN, 4-4